NWA3550

IEEE 802.11a/b/g Outdoor WLAN Access Point

User's Guide

Version 3.60
6/2008
Edition 2

DEFAULT LOGIN	
IP Address	**http://192.168.1.2**
Password	**1234**

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

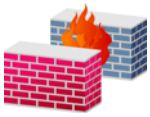
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NWA3550 may be referred to as the "ZyXEL Device", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Switch	Router

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- Please select an antenna that conforms with your local radio regulations. ZyXEL bears no responsibility whatsoever for cases of illegal installation.

This product is recyclable. Dispose of it properly.

Contents Overview

Introduction 31

Introducing the ZyXEL Device 33
Introducing the Web Configurator 43
Status Screens 47
Management Mode 51
Tutorial 55

The Web Configurator 83

System Screens 85
Wireless Configuration 91
Wireless Security Configuration 109
MBSSID and SSID 121
Other Wireless Configuration 129
IP Screen 141
Rogue AP 145
Remote Management Screens 151
Internal RADIUS Server 169
Certificates 177
Log Screens 195
VLAN 203
Maintenance 221

Troubleshooting and Specifications 231

Troubleshooting 233
Product Specifications 237

Appendices and Index 243

Table of Contents

About This User's Guide 3

Document Conventions 4

Safety Warnings 6

Contents Overview 9

Table of Contents 11

List of Figures 19

List of Tables 27

Part I: Introduction 31

Chapter 1
Introducing the ZyXEL Device 33

1.1 Introducing the ZyXEL Device 33
1.2 Applications for the ZyXEL Device 33
1.2.1 Access Point 34
1.2.2 Bridge / Repeater 34
1.2.3 AP + Bridge 35
1.2.4 MBSSID 36
1.2.5 Pre-Configured SSID Profiles 37
1.2.6 Configuring Dual WLAN Adaptors 37
1.3 CAPWAP 38
1.4 Ways to Manage the ZyXEL Device 39
1.5 Configuring Your ZyXEL Device's Security Features 39
1.5.1 Control Access to Your Device 39
1.5.2 Wireless Security 40
1.6 Maintaining Your ZyXEL Device 40
1.7 Hardware Connections 40

Chapter 2
Introducing the Web Configurator 43

2.1 Accessing the Web Configurator 43
2.2 Resetting the ZyXEL Device 44
2.2.1 Methods of Restoring Factory-Defaults 45

2.3 Navigating the Web Configurator 45

Chapter 3
Status Screens 47

3.1 The Status Screen 47

Chapter 4
Management Mode 51

4.1 About CAPWAP 51
4.1.1 CAPWAP Discovery and Management 52
4.1.2 CAPWAP and DHCP 52
4.1.3 CAPWAP and IP Subnets 52
4.1.4 Notes on CAPWAP 53
4.2 The Management Mode Screen 53

Chapter 5
Tutorial 55

5.1 How to Configure the Wireless LAN 55
5.1.1 Choosing the Wireless Mode 55
5.1.1.1 Configuring Dual WLAN Adaptors 56
5.1.2 Wireless LAN Configuration Overview 56
5.1.3 Further Reading 58
5.2 How to Configure Multiple Wireless Networks 58
5.2.1 Change the Operating Mode 59
5.2.2 Configure the VoIP Network 61
5.2.2.1 Set Up Security for the VoIP Profile 62
5.2.2.2 Activate the VoIP Profile 64
5.2.3 Configure the Guest Network 64
5.2.3.1 Set Up Security for the Guest Profile 65
5.2.3.2 Set up Layer 2 Isolation 66
5.2.3.3 Activate the Guest Profile 67
5.2.4 Testing the Wireless Networks 68
5.3 How to Set Up and Use Rogue AP Detection 68
5.3.1 Set Up and Save a Friendly AP list 70
5.3.2 Activate Periodic Rogue AP Detection 73
5.3.3 Set Up E-mail Logs 73
5.3.4 Configure Your Other Access Points 74
5.3.5 Test the Setup 75
5.4 Using Multiple MAC Filters and L-2 Isolation Profiles 75
5.4.1 Scenario 76
5.4.2 Your Requirements 76
5.4.3 Setup 76
5.4.4 Configure the SERVER_1 Network 77

5.4.5 Configure the SERVER_2 Network 79
5.4.6 Checking your Settings and Testing the Configuration 80
5.4.6.1 Checking Settings 80
5.4.6.2 Testing the Configuration 81

Part II: The Web Configurator 83

Chapter 6
System Screens 85

6.1 System Overview 85
6.2 Configuring General Setup 85
6.3 Administrator Authentication on RADIUS 86
6.3.1 Configuring the Password 86
6.4 Configuring Time Setting 88
6.5 Pre-defined NTP Time Servers List 90

Chapter 7
Wireless Configuration 91

7.1 Wireless Network Overview 91
7.2 Wireless LAN Basics 92
7.3 Quality of Service 92
7.3.1 WMM QoS 92
7.3.1.1 WMM QoS Priorities 93
7.3.2 ATC 93
7.3.3 ATC+WMM 94
7.3.3.1 ATC+WMM from LAN to WLAN 94
7.3.3.2 ATC+WMM from WLAN to LAN 94
7.3.4 Type Of Service (ToS) 95
7.3.4.1 DiffServ 95
7.3.4.2 DSCP and Per-Hop Behavior 95
7.3.5 ToS (Type of Service) and WMM QoS 95
7.4 Spanning Tree Protocol (STP) 96
7.4.1 Rapid STP 96
7.4.2 STP Terminology 96
7.4.3 How STP Works 97
7.4.4 STP Port States 97
7.5 DFS 97
7.6 Wireless Screen Overview 98
7.7 Configuring Wireless Settings 98
7.7.1 Access Point Mode 98
7.7.2 Bridge/Repeater Mode 101

7.7.3 AP+Bridge Mode 106
7.7.4 MBSSID Mode 108

Chapter 8
Wireless Security Configuration 109

8.1 Wireless Security Overview 109
8.1.1 SSID 109
8.1.2 MAC Address Filter 109
8.1.3 User Authentication 110
8.1.4 Encryption 110
8.2 Security Modes 111
8.3 Configuring Security 111
8.3.1 Security: WEP 112
8.3.2 Security: 802.1x Only 113
8.3.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit 114
8.3.4 Security: WPA 116
8.3.5 Security: WPA2 or WPA2-MIX 116
8.3.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX 118
8.4 Introduction to RADIUS 119
8.5 Configuring RADIUS 119

Chapter 9
MBSSID and SSID 121

9.1 Wireless LAN Infrastructures 121
9.1.1 MBSSID 121
9.1.2 Notes on Multiple BSS 121
9.1.3 Multiple BSS Example 121
9.1.4 Multiple BSS with VLAN Example 121
9.1.5 Configuring Multiple BSSs 122
9.2 SSID 125
9.2.1 The SSID Screen 125
9.2.2 Configuring SSID 127

Chapter 10
Other Wireless Configuration 129

10.1 Layer-2 Isolation Introduction 129
10.2 The Layer-2 Isolation Screen 130
10.3 Configuring Layer-2 Isolation 131
10.3.1 Layer-2 Isolation Examples 133
10.3.1.1 Layer-2 Isolation Example 1 133
10.3.1.2 Layer-2 Isolation Example 2 134
10.4 The MAC Filter Screen 134
10.4.1 Configuring MAC Filtering 135

10.5 Configuring Roaming 137
10.5.1 Requirements for Roaming 138

Chapter 11
IP Screen 141

11.1 Factory Ethernet Defaults 141
11.2 TCP/IP Parameters 141
11.2.1 WAN IP Address Assignment 141
11.3 Configuring IP Settings 142

Chapter 12
Rogue AP 145

12.1 Rogue AP Introduction 145
12.2 Rogue AP Examples 145
12.2.1 “Honeypot” Attack 146
12.3 Configuring Rogue AP Detection 147
12.3.1 Rogue AP: Configuration 147
12.3.2 Rogue AP: Friendly AP 148
12.3.3 Rogue AP List 149

Chapter 13
Remote Management Screens 151

13.1 Remote Management Overview 151
13.1.1 Remote Management Limitations 151
13.1.2 System Timeout 152
13.2 SSH 152
13.3 How SSH Works 152
13.4 SSH Implementation on the ZyXEL Device 153
13.4.1 Requirements for Using SSH 153
13.5 Configuring Telnet 153
13.6 Configuring FTP 155
13.7 WWW (HTTP and HTTPS) 156
13.8 Configuring WWW 157
13.9 HTTPS Example 158
13.9.1 Internet Explorer Warning Messages 158
13.9.2 Netscape Navigator Warning Messages 159
13.9.3 Avoiding the Browser Warning Messages 159
13.9.4 Login Screen 160
13.10 SNMP 162
13.10.1 Supported MIBs 164
13.10.2 SNMP Traps 164
13.11 SNMP Trap Interface Index 165
13.11.1 SNMP v3 and Security 165

13.11.2 Configuring SNMP 165
13.11.2.1 The SNMPv3 User Profile Screen 167

Chapter 14
Internal RADIUS Server 169

14.1 Internal RADIUS Overview 169
14.2 Internal RADIUS Server Setting 169
14.3 Trusted AP Overview 171
14.4 Configuring Trusted AP 172
14.5 Configuring Trusted Users 174

Chapter 15
Certificates 177

15.1 Certificates Overview 177
15.1.1 Advantages of Certificates 178
15.2 Self-signed Certificates 178
15.3 Verifying a Certificate 178
15.3.1 Checking the Fingerprint of a Certificate on Your Computer 178
15.4 Configuration Summary 179
15.5 My Certificates 179
15.6 Certificate File Formats 181
15.7 Importing a Certificate 182
15.8 Creating a Certificate 183
15.9 My Certificate Details 185
15.10 Trusted CAs 188
15.11 Importing a Trusted CA's Certificate 189
15.12 Trusted CA Certificate Details 190

Chapter 16
Log Screens 195

16.1 Configuring View Log 195
16.2 Configuring Log Settings 196
16.3 Example Log Messages 198
16.4 Log Commands 200
16.4.1 Configuring What You Want the ZyXEL Device to Log 200
16.4.2 Displaying Logs 200
16.5 Log Command Example 201

Chapter 17
VLAN 203

17.1 VLAN 203
17.1.1 Management VLAN ID 203
17.1.2 VLAN Tagging 203

17.2 Configuring VLAN 204
17.2.1 Wireless VLAN 204
17.2.2 RADIUS VLAN 206
17.2.3 Configuring Management VLAN Example 207
17.2.4 Configuring Microsoft's IAS Server Example 210
17.2.4.1 Configuring VLAN Groups 210
17.2.4.2 Configuring Remote Access Policies 211
17.2.5 Second Rx VLAN ID Example 218
17.2.5.1 Second Rx VLAN Setup Example 218

Chapter 18
Maintenance 221

18.1 Maintenance Overview 221
18.2 System Status Screen 221
18.2.1 System Statistics 222
18.3 Association List 223
18.4 Channel Usage 224
18.5 F/W Upload Screen 225
18.6 Configuration Screen 227
18.6.1 Backup Configuration 228
18.6.2 Restore Configuration 228
18.6.3 Back to Factory Defaults 230
18.7 Restart Screen 230

Part III: Troubleshooting and Specifications 231

Chapter 19
Troubleshooting 233

19.1 Power and Hardware Connections 233
19.2 ZyXEL Device Access and Login 233
19.3 Internet Access 235
19.4 Wireless Router/AP Troubleshooting 236

Chapter 20
Product Specifications 237

Part IV: Appendices and Index 243

Appendix A Setting Up Your Computer's IP Address 245

Appendix B Wireless LANs 269

Appendix C Pop-up Windows, JavaScripts and Java Permissions 283
Appendix D Importing Certificates 289
Appendix E IP Addresses and Subnetting 313
Appendix F Text File Based Auto Configuration 321
Appendix G Legal Information 329
Appendix H Customer Support 333
Index 339

List of Figures

Figure 1 Access Point Application 34
Figure 2 Bridge Application 35
Figure 3 Repeater Application 35
Figure 4 AP+Bridge Application 36
Figure 5 Multiple BSSs 37
Figure 6 Dual WLAN Adaptors Example 38
Figure 7 CAPWAP Network Example 39
Figure 8 Change Password Screen 44
Figure 9 Replace Certificate Screen 44
Figure 10 The Status Screen of the Web Configurator 45
Figure 11 The Status Screen 47
Figure 12 CAPWAP Network Example 51
Figure 13 CAPWAP and DHCP Option 43 53
Figure 14 The Management Mode Screen 53
Figure 15 Configuring Wireless LAN 57
Figure 16 Tutorial: Example MBSSID Setup 59
Figure 17 Tutorial: Wireless LAN: Before 60
Figure 18 Tutorial: Wireless LAN: Change Mode 60
Figure 19 Tutorial: WIRELESS > SSID 61
Figure 20 Tutorial: VoIP SSID Profile Edit 62
Figure 21 Tutorial: VoIP Security 63
Figure 22 Tutorial: VoIP Security Profile Edit 63
Figure 23 Tutorial: VoIP Security: Updated 64
Figure 24 Tutorial: Activate VoIP Profile 64
Figure 25 Tutorial: Guest Edit 65
Figure 26 Tutorial: Guest Security Profile Edit 65
Figure 27 Tutorial: Guest Security: Updated 66
Figure 28 Tutorial: Layer 2 Isolation 66
Figure 29 Tutorial: Layer 2 Isolation Profile 67
Figure 30 Tutorial: Activate Guest Profile 68
Figure 31 Tutorial: Wireless Network Example 69
Figure 32 Tutorial: Friendly AP (Before Data Entry) 70
Figure 33 Tutorial: Friendly AP (After Data Entry) 71
Figure 34 Tutorial: Configuration 72
Figure 35 Tutorial: Warning 72
Figure 36 Tutorial: Save Friendly AP list 72
Figure 37 Tutorial: Periodic Rogue AP Detection 73
Figure 38 Tutorial: Log Settings 74

Figure 39 Tutorial: Example Network 76
Figure 40 Tutorial: SSID Profile 78
Figure 41 Tutorial: SSID Edit 78
Figure 42 Tutorial: Layer-2 Isolation Edit 79
Figure 43 Tutorial: MAC Filter Edit (SERVER_1) 79
Figure 44 Tutorial: SSID Profiles Activated 81
Figure 45 Tutorial: SSID Tab Correct Settings 81
Figure 46 System > General 85
Figure 47 SYSTEM > Password. 87
Figure 48 SYSTEM > Time Setting 88
Figure 49 Example of a Wireless Network 91
Figure 50 DiffServ: Differentiated Service Field 95
Figure 51 Wireless: Access Point 99
Figure 52 Bridging Example 102
Figure 53 Bridge Loop: Two Bridges Connected to Hub 102
Figure 54 Bridge Loop: Bridge Connected to Wired LAN 103
Figure 55 Wireless: Bridge/Repeater 104
Figure 56 Wireless: AP+Bridge 107
Figure 57 Wireless > Security 112
Figure 58 WIRELESS > Security: WEP 113
Figure 59 Security: 802.1x Only 114
Figure 60 Security: 802.1x Static 64-bit, 802.1x Static 128-bit 115
Figure 61 Security: WPA 116
Figure 62 Security:WPA2 or WPA2-MIX 117
Figure 63 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX 118
Figure 64 RADIUS 119
Figure 65 Multiple BSS with VLAN Example 122
Figure 66 Wireless: Multiple BSS 123
Figure 67 SSID 126
Figure 68 Configuring SSID 127
Figure 69 Layer-2 Isolation Application 130
Figure 70 WIRELESS > Layer 2 Isolation 131
Figure 71 WIRELESS > Layer-2 Isolation Configuration Screen 132
Figure 72 Layer-2 Isolation Example Configuration 133
Figure 73 Layer-2 Isolation Example 1 133
Figure 74 Layer-2 Isolation Example 2 134
Figure 75 WIRELESS > MAC Filter 135
Figure 76 MAC Address Filter 136
Figure 77 Roaming Example 138
Figure 78 Roaming 139
Figure 79 IP Setup 142
Figure 80 Rogue AP: Example 146
Figure 81 “Honeypot” Attack 147

Figure 82 ROGUE AP > Configuration 148
Figure 83 ROGUE AP > Friendly AP 149
Figure 84 ROGUE AP > Rogue AP 150
Figure 85 How SSH Works 152
Figure 86 Remote Management: Telnet 154
Figure 87 Remote Management: FTP 155
Figure 88 HTTPS Implementation 156
Figure 89 Remote Management: WWW 157
Figure 90 Security Alert Dialog Box (Internet Explorer) 158
Figure 91 Security Certificate 1 (Netscape) 159
Figure 92 Security Certificate 2 (Netscape) 159
Figure 93 Example: Lock Denoting a Secure Connection 161
Figure 94 Replace Certificate 161
Figure 95 Device-specific Certificate 162
Figure 96 Common ZyXEL Device Certificate 162
Figure 97 SNMP Management Model 163
Figure 98 Remote Management: SNMP 166
Figure 99 Remote Management: SNMPv3 User Profile 167
Figure 100 Internal RADIUS Server Setting Screen 170
Figure 101 Trusted AP Overview 172
Figure 102 Trusted AP Screen 173
Figure 103 Trusted Users Screen 174
Figure 104 Certificates on Your Computer 178
Figure 105 Certificate Details 179
Figure 106 My Certificates 180
Figure 107 My Certificate Import 182
Figure 108 My Certificate Create 183
Figure 109 My Certificate Details 186
Figure 110 Trusted CAs 188
Figure 111 Trusted CA Import 190
Figure 112 Trusted CA Details 191
Figure 113 View Log 195
Figure 114 Log Settings 197
Figure 115 Wireless VLAN 205
Figure 116 RADIUS VLAN 206
Figure 117 Management VLAN Configuration Example 208
Figure 118 VLAN-Aware Switch - Static VLAN 208
Figure 119 VLAN-Aware Switch 208
Figure 120 VLAN-Aware Switch - VLAN Status 209
Figure 121 VLAN Setup 209
Figure 122 New Global Security Group 211
Figure 123 Add Group Members 211
Figure 124 New Remote Access Policy for VLAN Group 212

Figure 125 Specifying Windows-Group Condition 212
Figure 126 Adding VLAN Group 213
Figure 127 Granting Permissions and User Profile Screens 213
Figure 128 Authentication Tab Settings 214
Figure 129 Encryption Tab Settings 214
Figure 130 Connection Attributes Screen 215
Figure 131 RADIUS Attribute Screen 215
Figure 132 802 Attribute Setting for Tunnel-Medium-Type 216
Figure 133 VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID 216
Figure 134 VLAN Attribute Setting for Tunnel-Type 217
Figure 135 Completed Advanced Tab 217
Figure 136 Second Rx VLAN ID Example 218
Figure 137 Configuring SSID: Second Rx VLAN ID Example 219
Figure 138 System Status 221
Figure 139 System Status: Show Statistics 222
Figure 140 Association List 224
Figure 141 Channel Usage 225
Figure 142 Firmware Upload 226
Figure 143 Firmware Upload In Process 226
Figure 144 Network Temporarily Disconnected 227
Figure 145 Firmware Upload Error 227
Figure 146 Configuration 228
Figure 147 Configuration Upload Successful 229
Figure 148 Network Temporarily Disconnected 229
Figure 149 Configuration Upload Error 229
Figure 150 Reset Warning Message 230
Figure 151 Restart Screen 230
Figure 152 Windows XP: Start Menu 246
Figure 153 Windows XP: Control Panel 246
Figure 154 Windows XP: Control Panel > Network Connections > Properties 246
Figure 155 Windows XP: Local Area Connection Properties 247
Figure 156 Windows XP: Internet Protocol (TCP/IP) Properties 248
Figure 157 Windows Vista: Start Menu 249
Figure 158 Windows Vista: Control Panel 249
Figure 159 Windows Vista: Network And Internet 249
Figure 160 Windows Vista: Network and Sharing Center 250
Figure 161 Windows Vista: Network and Sharing Center 250
Figure 162 Windows Vista: Local Area Connection Properties 251
Figure 163 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties 252
Figure 164 Mac OS X 10.4: Apple Menu 253
Figure 165 Mac OS X 10.4: System Preferences 253
Figure 166 Mac OS X 10.4: Network Preferences 254
Figure 167 Mac OS X 10.4: Network Preferences > TCP/IP Tab. 254

Figure 168 Mac OS X 10.4: Network Preferences > Ethernet 255
Figure 169 Mac OS X 10.4: Network Utility 255
Figure 170 Mac OS X 10.5: Apple Menu 256
Figure 171 Mac OS X 10.5: Systems Preferences 256
Figure 172 Mac OS X 10.5: Network Preferences > Ethernet 257
Figure 173 Mac OS X 10.5: Network Preferences > Ethernet 258
Figure 174 Mac OS X 10.5: Network Utility 258
Figure 175 Ubuntu 8: System > Administration Menu 259
Figure 176 Ubuntu 8: Network Settings > Connections 259
Figure 177 Ubuntu 8: Administrator Account Authentication 260
Figure 178 Ubuntu 8: Network Settings > Connections 260
Figure 179 Ubuntu 8: Network Settings > Properties 261
Figure 180 Ubuntu 8: Network Settings > DNS 261
Figure 181 Ubuntu 8: Network Tools 262
Figure 182 openSUSE 10.3: K Menu > Computer Menu 263
Figure 183 openSUSE 10.3: K Menu > Computer Menu 263
Figure 184 openSUSE 10.3: YaST Control Center 264
Figure 185 openSUSE 10.3: Network Settings 264
Figure 186 openSUSE 10.3: Network Card Setup 265
Figure 187 openSUSE 10.3: Network Settings 266
Figure 188 openSUSE 10.3: KNetwork Manager 266
Figure 189 openSUSE: Connection Status - KNetwork Manager 267
Figure 190 Peer-to-Peer Communication in an Ad-hoc Network 269
Figure 191 Basic Service Set 270
Figure 192 Infrastructure WLAN 271
Figure 193 RTS/CTS 272
Figure 194 WPA(2) with RADIUS Application Example 279
Figure 195 WPA(2)-PSK Authentication 280
Figure 196 Pop-up Blocker 283
Figure 197 Internet Options: Privacy 284
Figure 198 Internet Options: Privacy 285
Figure 199 Pop-up Blocker Settings 285
Figure 200 Internet Options: Security 286
Figure 201 Security Settings - Java Scripting 287
Figure 202 Security Settings - Java 287
Figure 203 Java (Sun) 288
Figure 204 Internet Explorer 7: Certification Error 290
Figure 205 Internet Explorer 7: Certification Error 290
Figure 206 Internet Explorer 7: Certificate Error 290
Figure 207 Internet Explorer 7: Certificate 291
Figure 208 Internet Explorer 7: Certificate Import Wizard 291
Figure 209 Internet Explorer 7: Certificate Import Wizard 292
Figure 210 Internet Explorer 7: Certificate Import Wizard 292

Figure 211 Internet Explorer 7: Select Certificate Store 292
Figure 212 Internet Explorer 7: Certificate Import Wizard 293
Figure 213 Internet Explorer 7: Security Warning 293
Figure 214 Internet Explorer 7: Certificate Import Wizard 293
Figure 215 Internet Explorer 7: Website Identification 294
Figure 216 Internet Explorer 7: Public Key Certificate File 294
Figure 217 Internet Explorer 7: Open File - Security Warning 295
Figure 218 Internet Explorer 7: Tools Menu 295
Figure 219 Internet Explorer 7: Internet Options 296
Figure 220 Internet Explorer 7: Certificates 296
Figure 221 Internet Explorer 7: Certificates 297
Figure 222 Internet Explorer 7: Root Certificate Store 297
Figure 223 Firefox 2: Website Certified by an Unknown Authority 297
Figure 224 Firefox 2: Page Info 298
Figure 225 Firefox 2: Tools Menu 298
Figure 226 Firefox 2: Options 299
Figure 227 Firefox 2: Certificate Manager 299
Figure 228 Firefox 2: Select File 300
Figure 229 Firefox 2: Tools Menu 300
Figure 230 Firefox 2: Options 301
Figure 231 Firefox 2: Certificate Manager 301
Figure 232 Firefox 2: Delete Web Site Certificates 302
Figure 233 Opera 9: Certificate signer not found 302
Figure 234 Opera 9: Security information 303
Figure 235 Opera 9: Tools Menu 303
Figure 236 Opera 9: Preferences 304
Figure 237 Opera 9: Certificate manager 304
Figure 238 Opera 9: Import certificate 305
Figure 239 Opera 9: Install authority certificate 305
Figure 240 Opera 9: Install authority certificate 306
Figure 241 Opera 9: Tools Menu 306
Figure 242 Opera 9: Preferences 307
Figure 243 Opera 9: Certificate manager 308
Figure 244 Konqueror 3.5: Server Authentication 309
Figure 245 Konqueror 3.5: Server Authentication 309
Figure 246 Konqueror 3.5: KDE SSL Information 309
Figure 247 Konqueror 3.5: Public Key Certificate File 310
Figure 248 Konqueror 3.5: Certificate Import Result 310
Figure 249 Konqueror 3.5: Kleopatra 310
Figure 250 Konqueror 3.5: Settings Menu 311
Figure 251 Konqueror 3.5: Configure 311
Figure 252 Network Number and Host ID 314
Figure 253 Subnetting Example: Before Subnetting 316

Figure 254 Subnetting Example: After Subnetting 317
Figure 255 Text File Based Auto Configuration 321
Figure 256 Configuration File Format 323
Figure 257 WEP Configuration File Example 324
Figure 258 802.1X Configuration File Example 325
Figure 259 WPA-PSK Configuration File Example 325
Figure 260 WPA Configuration File Example 326
Figure 261 Wlan Configuration File Example 327

List of Tables

Table 1 The Status Screen 47
Table 2 The Management Mode Screen 54
Table 3 Tutorial: Example Information 59
Table 4 Tutorial: Rogue AP Example Information 69
Table 5 Tutorial: Friendly AP Information 71
Table 6 Tutorial: SSID Profile Security Settings 76
Table 7 Tutorial: Example Network MAC Addresses 77
Table 8 Tutorial: Example User MAC Addresses 77
Table 9 Tutorial: SERVER_2 Network Information 80
Table 10 System > General 85
Table 11 Password 87
Table 12 SYSTEM > Time Setting 89
Table 13 Default Time Servers 90
Table 14 WMM QoS Priorities 93
Table 15 Typical Packet Sizes 93
Table 16 Automatic Traffic Classifier Priorities 93
Table 17 ATC + WMM Priority Assignment (LAN to WLAN) 94
Table 18 ATC + WMM Priority Assignment (WLAN to LAN) 94
Table 19 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping 96
Table 20 STP Path Costs 96
Table 21 STP Port States 97
Table 22 Wireless: Access Point 99
Table 23 Wireless: Bridge/Repeater 104
Table 24 Types of Encryption for Each Type of Authentication 110
Table 25 Security Modes 111
Table 26 WIRELESS > Security 112
Table 27 Security: WEP 113
Table 28 Security: 802.1x Only 114
Table 29 Security: 802.1x Static 64-bit, 802.1x Static 128-bit 115
Table 30 Security: WPA 116
Table 31 Security: WPA2 or WPA2-MIX 117
Table 32 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX 118
Table 33 RADIUS 120
Table 34 Wireless: Multiple BSS 123
Table 35 SSID 126
Table 36 Configuring SSID 127
Table 37 WIRELESS > Layer-2 Isolation 131
Table 38 WIRELESS > Layer-2 Isolation Configuration 132

Table 39 WIRELESS > MAC Filter 135
Table 40 MAC Address Filter 136
Table 41 Private IP Address Ranges 141
Table 42 IP Setup 142
Table 43 ROGUE AP > Configuration 148
Table 44 ROGUE AP > Friendly AP 149
Table 45 ROGUE AP > Rogue AP 150
Table 46 Remote Management Overview 151
Table 47 Remote Management: Telnet 154
Table 48 Remote Management: FTP 155
Table 49 Remote Management: WWW 157
Table 50 SNMP Traps 164
Table 51 SNMP Interface Index to Physical and Virtual Port Mapping 165
Table 52 Remote Management: SNMP 166
Table 53 Remote Management: SNMP User Profile 167
Table 54 Internal RADIUS Server Setting Screen Setting 170
Table 55 Trusted AP 173
Table 56 Trusted Users 174
Table 57 My Certificates 180
Table 58 My Certificate Import 183
Table 59 My Certificate Create 184
Table 60 My Certificate Details 186
Table 61 Trusted CAs 189
Table 62 Trusted CA Import 190
Table 63 Trusted CA Details 191
Table 64 View Log 195
Table 65 Log Settings 197
Table 66 System Maintenance Logs 198
Table 67 ICMP Notes 199
Table 68 Sys log 200
Table 69 Log Categories and Available Settings Example 200
Table 70 Wireless VLAN 205
Table 71 RADIUS VLAN 207
Table 72 Standard RADIUS Attributes 210
Table 73 System Status 221
Table 74 System Status: Show Statistics 223
Table 75 Association List 224
Table 76 Channel Usage 225
Table 77 Firmware Upload 226
Table 78 Restore Configuration 228
Table 79 Hardware Specifications 237
Table 80 Firmware Specifications 238
Table 81 ZyXEL Device Compatible Antennas 240

Table 82 ZyXEL Device Compatible Antenna Cables 240
Table 83 Power over Ethernet Injector Specifications 241
Table 84 Power over Ethernet Injector RJ-45 Port Pin Assignments 241
Table 85 IEEE 802.11g 273
Table 86 Wireless Security Levels 274
Table 87 Comparison of EAP Authentication Types 277
Table 88 Wireless Security Relational Matrix 280
Table 89 Subnet Masks 314
Table 90 Subnet Masks 315
Table 91 Maximum Host Numbers 315
Table 92 Alternative Subnet Mask Notation 315
Table 93 Subnet 1 317
Table 94 Subnet 2 318
Table 95 Subnet 3 318
Table 96 Subnet 4 318
Table 97 Eight Subnets 318
Table 98 24-bit Network Number Subnet Planning 319
Table 99 16-bit Network Number Subnet Planning 319
Table 100 Auto Configuration by DHCP 322
Table 101 Manual Configuration 322
Table 102 Configuration via SNMP 323
Table 103 Displaying the File Version 323
Table 104 Displaying the File Version 323
Table 105 Displaying the Auto Configuration Status 324

PART I
Introduction

Introducing the ZyXEL Device (33)
Introducing the Web Configurator (43)
Status Screens (47)
Tutorial (55)

1

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Introducing the ZyXEL Device

Your ZyXEL Device extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

It is highly versatile, supporting multiple BSSIDs simultaneously. The Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

Multiple security profiles allow you to easily assign different types of security to groups of users. The ZyXEL Device controls network access with MAC address filtering, rogue AP detection, layer 2 isolation and an internal authentication server. It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access (WPA), WPA2 and WEP data encryption.

Your ZyXEL Device is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance.

See the Quick Start Guide for instructions on how to make hardware connections.

1.2 Applications for the ZyXEL Device

The ZyXEL Device can be configured to use the following WLAN operating modes

1. Access Point (AP)
2. Bridge/Repeater
3. AP+Bridge
4. MBSSID

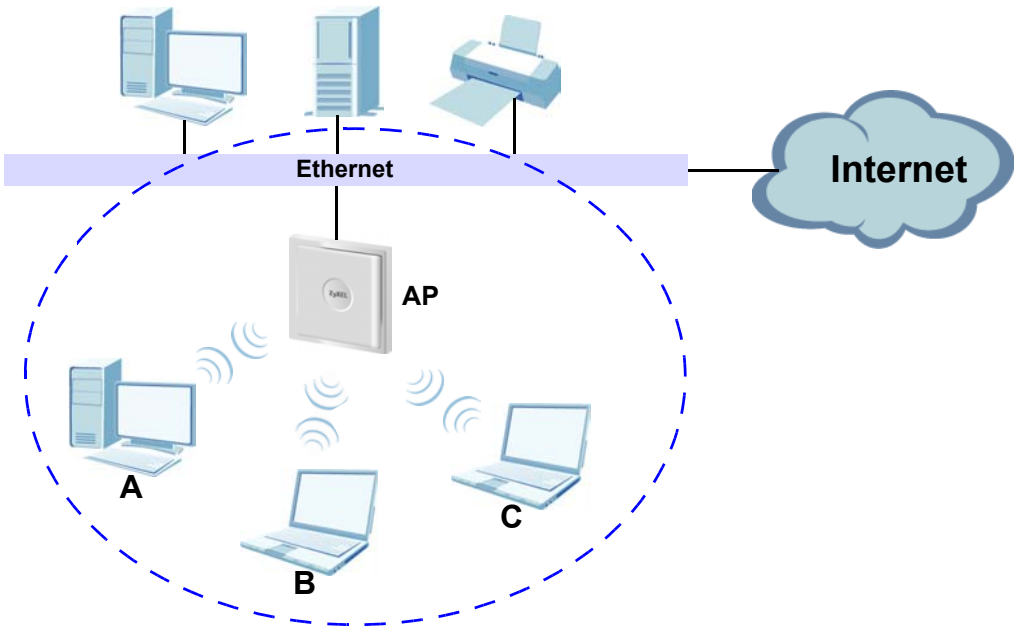
Applications for each operating mode are shown below.

A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

1.2.1 Access Point

The ZyXEL Device is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyXEL Device is shown as follows. Clients **A**, **B** and **C** can access the wired network through the ZyXEL Devices.

Figure 1 Access Point Application



1.2.2 Bridge / Repeater

The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. In the figure below, the two ZyXEL Devices (**A** and **B**) are connected to independent wired networks and have a bridge connection (**A** can communicate with **B**) at the same time. A ZyXEL Device in repeater mode (**C**) has no Ethernet connection. When the ZyXEL Device is in bridge mode, you should enable STP to prevent bridge loops.

When the ZyXEL Device is in **Bridge / Repeater** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See Section 7.7.2 on page 101 for more details.

Once the security settings of peer sides match one another, the connection between devices is made.

At the time of writing, WDS security is compatible with other ZyXEL access points only. Refer to your other access point's documentation for details.

Figure 2 Bridge Application

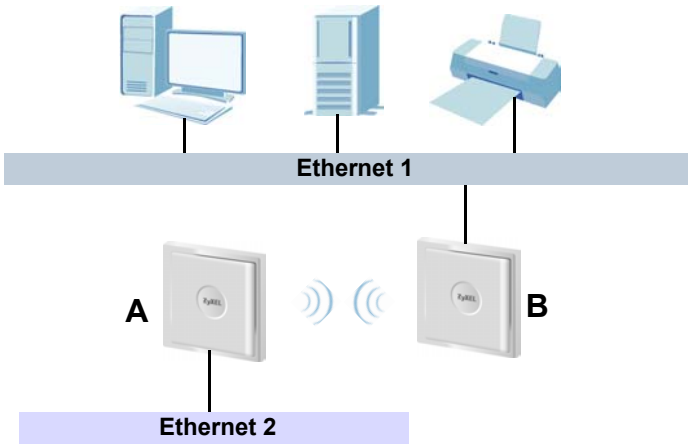
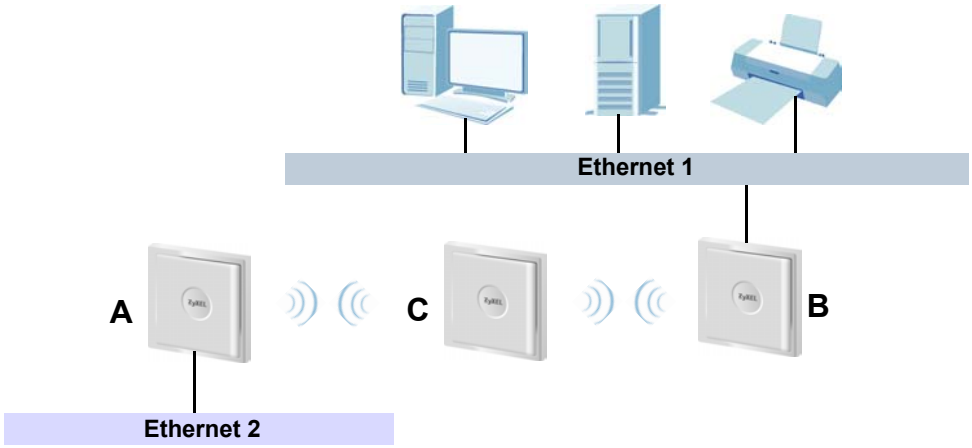


Figure 3 Repeater Application



1.2.3 AP + Bridge

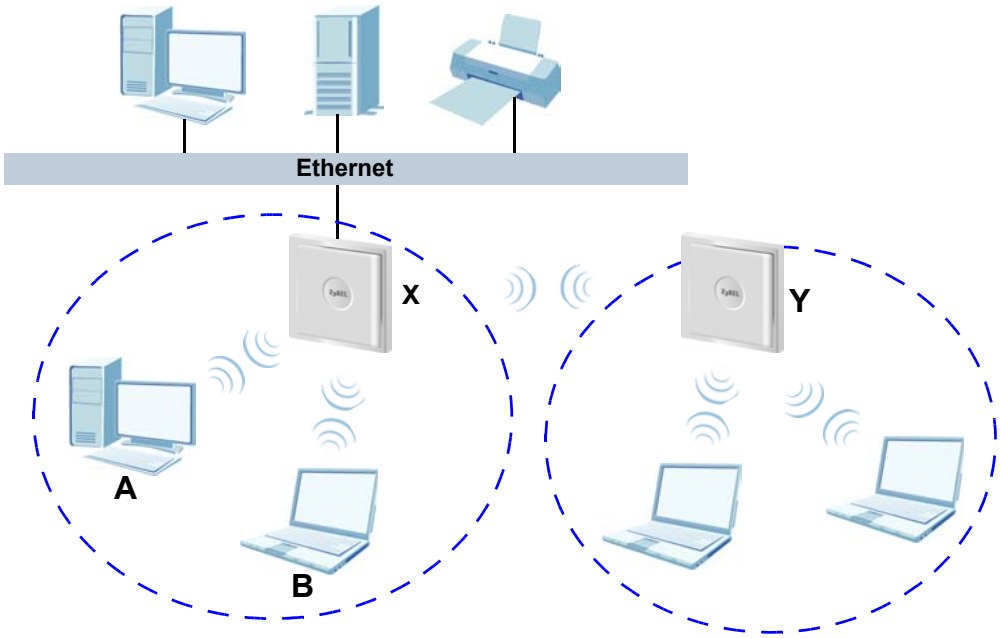
In **AP+Bridge** mode, the ZyXEL Device supports both AP and bridge connection at the same time.

In the figure below, **A** and **B** use **X** as an **AP** to access the wired network, while **X** and **Y** communicate in bridge mode.

When the ZyXEL Device is in **AP + Bridge** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See Section 7.7.3 on page 106 for more details.

Unless specified, the term “security settings” refers to the traffic between the wireless stations and the ZyXEL Device.

Figure 4 AP+Bridge Application



1.2.4 MBSSID

A BSS (Basic Service Set) is the set of devices forming a single wireless network (usually an access point and one or more wireless clients). An SSID (Service Set IDentifier) is the name of a BSS. In MBSSID (Multiple BSS) mode, the ZyXEL Device provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile.

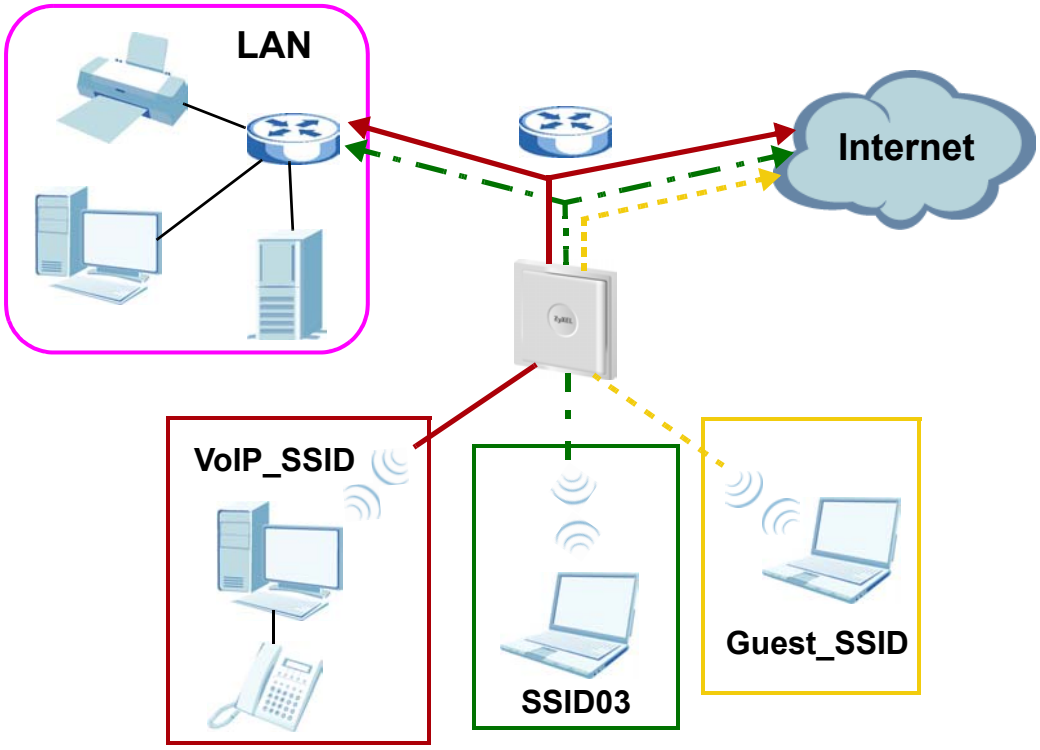
You can configure up to sixteen SSID profiles, and have up to eight active at any one time.

You can assign different wireless and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs.

To the wireless clients in the network, each SSID appears to be a different access point. As in any wireless network, clients can associate only with the SSIDs for which they have the correct security settings.

For example, you might want to set up a wireless network in your office where Internet telephony (Voice over IP, or VoIP) users have priority. You also want a regular wireless network for standard users, as well as a 'guest' wireless network for visitors. In the following figure, **VoIP_SSID** users have Quality of Service (QoS) priority, **SSID03** is the wireless network for standard users, and **Guest_SSID** is the wireless network for guest users. In this example, the guest user is forbidden access to the wired LAN behind the AP and can access only the Internet.

Figure 5 Multiple BSSs



1.2.5 Pre-Configured SSID Profiles

The ZyXEL Device has two pre-configured SSID profiles.

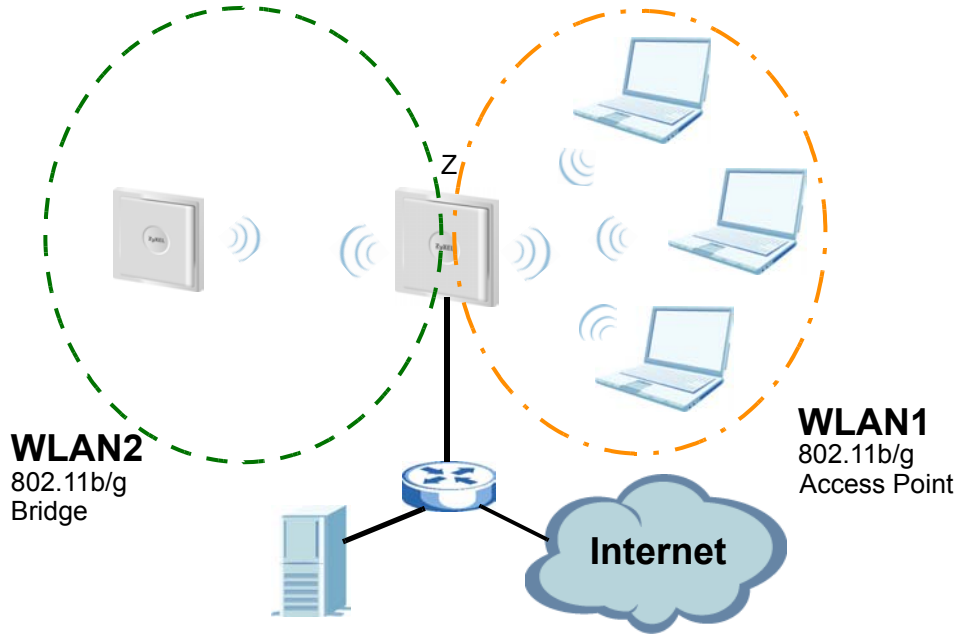
1. **VoIP_SSID**. This profile is intended for use by wireless clients requiring the highest QoS (Quality of Service) level for VoIP (Voice over IP) telephony and other applications requiring low latency. The QoS level of this profile is not user-configurable. See Chapter 7 on page 91 for more information on QoS.
2. **Guest_SSID**. This profile is intended for use by visitors and others who require access to certain resources on the network (an Internet gateway or a network printer, for example) but must not have access to the rest of the network. Layer 2 isolation is enabled (see Section 10.1 on page 129), and QoS is set to **NONE**. Intra-BSS traffic blocking is also enabled (see Section 9.2 on page 125). These fields are all user-configurable.

1.2.6 Configuring Dual WLAN Adaptors

The ZyXEL Device is equipped with dual wireless adaptors. This means you can configure two different wireless networks to operate simultaneously.

In the following example, the ZyXEL Device (**Z**) uses **WLAN1** in **Access Point** mode to allow IEEE 802.11b and IEEE 802.11g clients to access the wired network, and **WLAN2** in **AP+Bridge** mode to allow an IEEE 802.11a AP to communicate with the wired network.

Figure 6 Dual WLAN Adaptors Example



1.3 CAPWAP

The ZyXEL Device supports CAPWAP (Control And Provisioning of Wireless Access Points). This is ZyXEL's implementation of the IETF's (Internet Engineering Task Force) CAPWAP protocol.

ZyXEL's CAPWAP allows a single access point to manage up to eight other access points. The managed APs receive all their configuration information from the controller AP. The CAPWAP dataflow is protected by DTLS (Datagram Transport Layer Security).

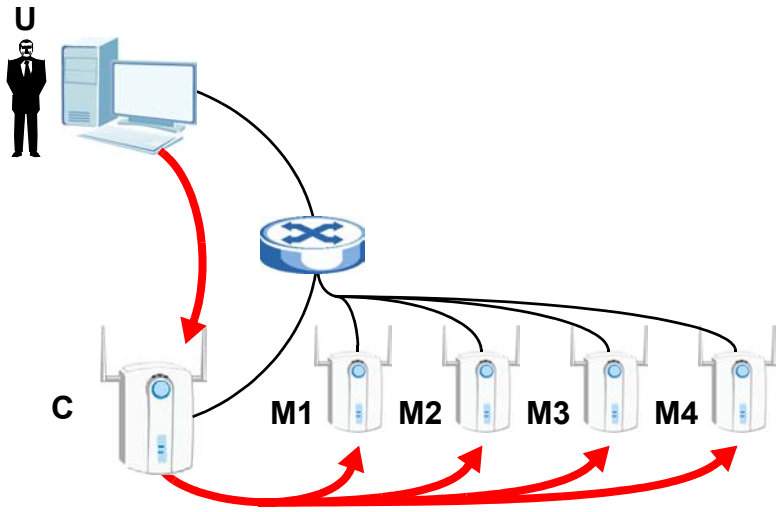
At the time of writing, the NWA-3160 is the only ZyXEL AP model that can be a CAPWAP controller.

At the time of writing, the following ZyXEL AP models can be CAPWAP managed APs:

- NWA-3160
- NWA-3163
- NWA-3500
- NWA-3550
- NWA-8500

The following figure illustrates a CAPWAP wireless network. The user (**U**) configures the controller AP (**C**), which then automatically updates the configurations of the managed APs (**M1** ~ **M4**).

Figure 7 CAPWAP Network Example



1.4 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device. Use Telnet to access the SMT.
- FTP for firmware upgrades and configuration backup and restore.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.5 Configuring Your ZyXEL Device's Security Features

Your ZyXEL Device comes with a variety of security features. This section summarizes these features and provides links to sections in the User's Guide to configure security settings on your ZyXEL Device. Follow the suggestions below to improve security on your ZyXEL Device and network.

1.5.1 Control Access to Your Device

Ensure only people with permission can access your ZyXEL Device.

- Control physical access by locating devices in secure areas, such as locked rooms. Most ZyXEL Devices have a reset button. If an unauthorized person has access to the reset button, they can then reset the device's password to its default password, log in and reconfigure its settings.

- Change any default passwords on the ZyXEL Device, such as the password used for accessing the ZyXEL Device's web configurator (if it has a web configurator). Use a password with a combination of letters and numbers and change your password regularly. Write down the password and put it in a safe place.
- Avoid setting a long timeout period before the ZyXEL Device's web configurator automatically times out. A short timeout reduces the risk of unauthorized person accessing the web configurator while it is left idle.

See Chapter 6 on page 85 for instructions on changing your password and setting the timeout period.

- Configure remote management to control who can manage your ZyXEL Device. See Chapter 13 on page 151 for more information. If you enable remote management, ensure you have enabled remote management only on the IP addresses, services or interfaces you intended and that other remote management settings are disabled.

1.5.2 Wireless Security

Wireless devices are especially vulnerable to attack. If your ZyXEL Device has a wireless function, take the following measures to improve wireless security.

- Enable wireless security on your ZyXEL Device. Choose the most secure encryption method that all devices on your network support. See Section 8.3 on page 111 for directions on configuring encryption. If you have a RADIUS server, enable IEEE 802.1x or WPA(2) user identification on your network so users must log in. This method is more common in business environments.
- Hide your wireless network name (SSID). The SSID can be regularly broadcast and unauthorized users may use this information to access your network. See Section 9.2 on page 125 for directions on using the web configurator to hide the SSID.
- Enable the MAC filter to allow only trusted users to access your wireless network or deny unwanted users access based on their MAC address. See Section 10.4 on page 134 for directions on configuring the MAC filter.

1.6 Maintaining Your ZyXEL Device

Do the following things regularly to keep your ZyXEL Device running.

- Check the ZyXEL website (www.zyxel.com.tw) regularly for new firmware for your ZyXEL Device. Ensure you download the correct firmware for your model.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

1.7 Hardware Connections

See your Quick Start Guide for information on making hardware connections.

Your ZyXEL Device has two wireless LAN adaptors, WLAN1 and WLAN2. WLAN1 uses the **RF1** antenna and WLAN2 uses the **RF2** antenna. If you connect only one antenna, you can use only the associated wireless LAN adaptor.

2

Introducing the Web Configurator

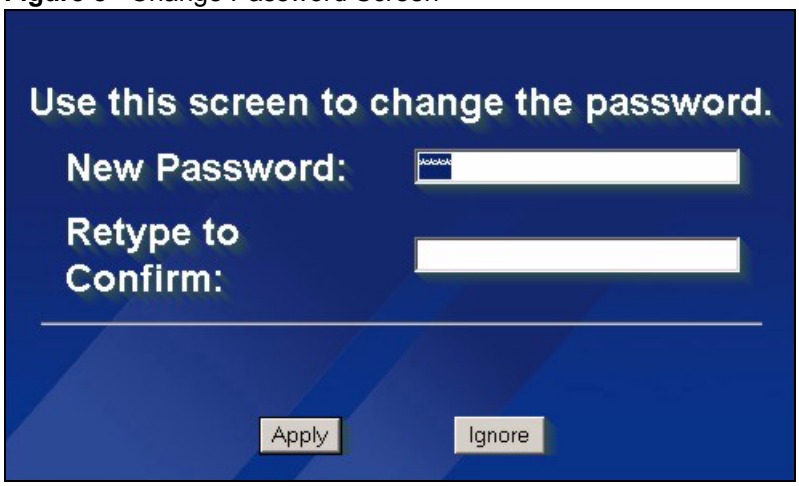
This chapter describes how to access the ZyXEL Device's web configurator and provides an overview of its screens.

2.1 Accessing the Web Configurator

1. Make sure your hardware is properly connected and prepare your computer or computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.2" as the URL (default).
4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
5. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) then click **Apply**. Alternatively, click **Ignore**.

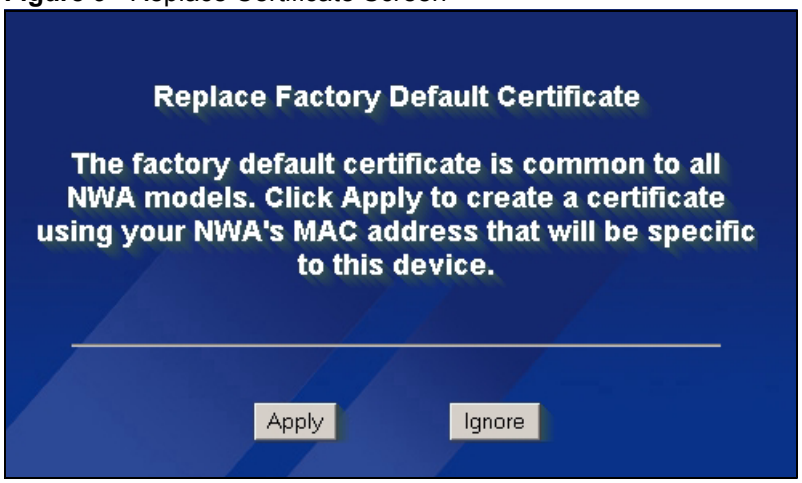
If you do not change the password, the following screen appears every time you login.

Figure 8 Change Password Screen



6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device.

Figure 9 Replace Certificate Screen



You should now see the **Status** screen. See Chapter 2 on page 43 for details about the **Status** screen.

The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyXEL Device if this happens.

2.2 Resetting the ZyXEL Device

This replaces the current configuration file with the factory-default configuration file. This means that you will lose all the settings you previously configured. The password will be reset to 1234.

2.2.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in the following ways:

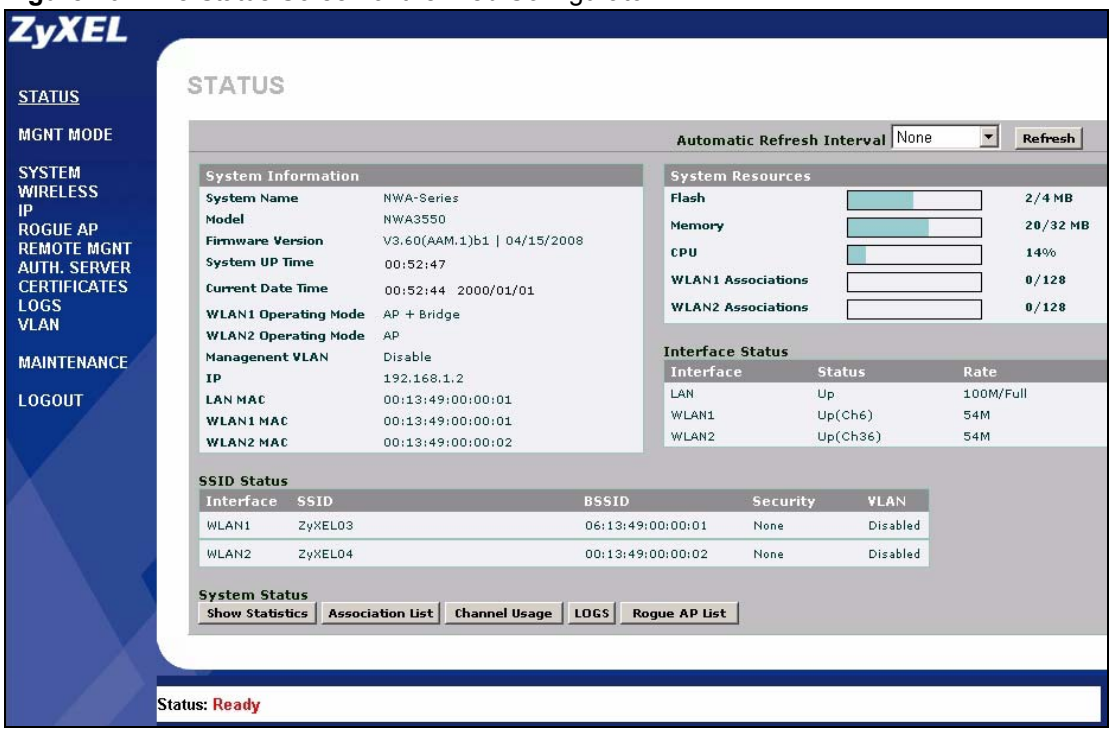
- Use the web configurator to restore defaults (refer to Chapter 18 on page 221).
- Transfer the configuration file to your ZyXEL Device using FTP. See the section on SMT configuration for more information.

2.3 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen.

- Click **LOGOUT** at any time to exit the web configurator.
- Check the status bar at the bottom of the screen when you click **Apply** or **OK** to verify that the configuration has been updated.

Figure 10 The Status Screen of the Web Configurator



- Click the links on the left of the screen to configure advanced features such as **MGNT MODE** (Standalone AP or Managed AP), **SYSTEM** (General, Password and Time Setting), **WIRELESS** (Wireless, SSID, Security, RADIUS, Layer-2 Isolation, MAC Filter), **IP**, **ROGUE AP** (Configuration, Friendly AP, Rogue AP), **REMOTE MGNT** (Telnet, FTP, WWW and SNMP), **AUTH. SERVER** (Setting, Trusted AP, Trusted Users), **CERTIFICATES** (My Certificates, Trusted CAs), **LOGS** (View Log and Log Settings) and **VLAN** (Wireless VLAN and RADIUS VLAN).
- Click **MAINTENANCE** to view information about your ZyXEL Device or upgrade configuration and firmware files. Maintenance features include **Status** (Statistics), **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore and Default) and **Restart**.

3

Status Screens

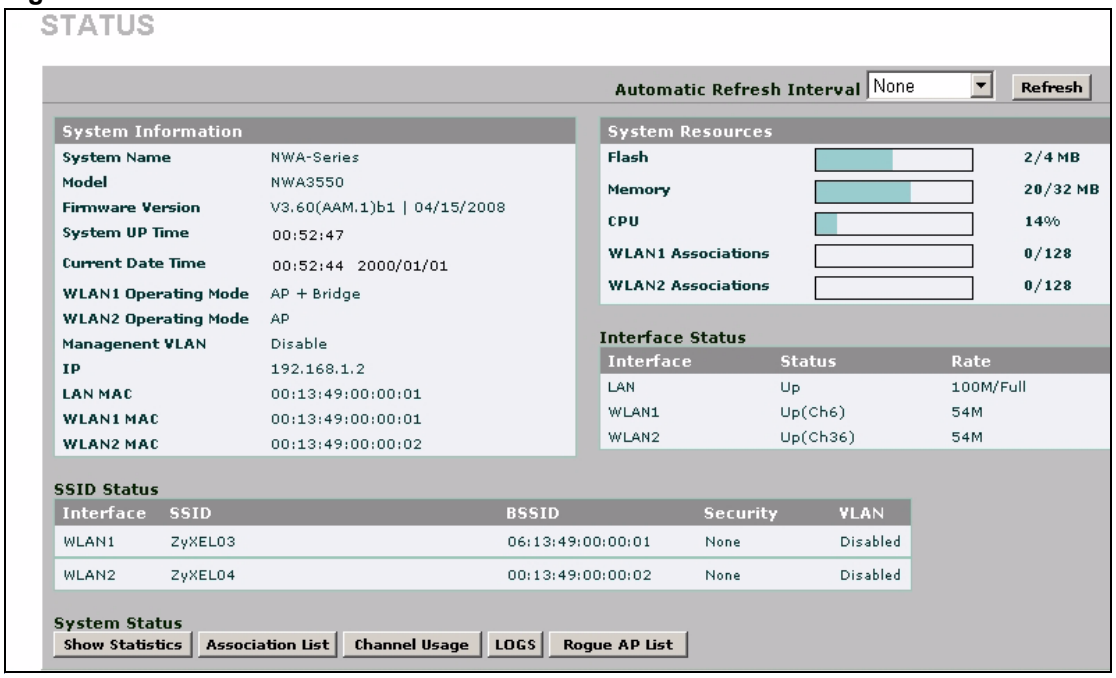
The **Status** screen displays when you log into the ZyXEL Device, or click **STATUS** in the navigation menu.

Use the **Status** screens to look at the current status of the device, system resources, interfaces and SSID status. The **Status** screen also provides detailed information about associated wireless clients, channel usage, logs and detected rogue APs.

3.1 The Status Screen

Cluck **Status**. The following screen displays.

Figure 11 The Status Screen



The following table describes the labels in this screen.

Table 1 The Status Screen

LABEL	DESCRIPTION
Automatic Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Refresh	Click this to update this screen immediately.

Table 1 The Status Screen

LABEL	DESCRIPTION
System Information	
System Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the **System > General** screen's **System Name** field.
Model	This field displays the ZyXEL Device's exact model name.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in **Maintenance > F/W Upload**.
System Up Time	This field displays the elapsed time since the ZyXEL Device was turned on.
Current Date Time	This field displays the date and time configured on the ZyXEL Device. You can change this in the **System** > **Time Setting** screen.
WLAN1 Operating Mode	This field displays the current operating mode of the first wireless module (**AP**, **Bridge / Repeater**, **AP + Bridge** or **MBSSID**). You can change the operating mode in the **Wireless** > **Wireless** screen.
WLAN2 Operating Mode	This field displays the current operating mode of the second wireless module (**AP**, **Bridge / Repeater**, **AP + Bridge** or **MBSSID**). You can change the operating mode in the **Wireless** > **Wireless** screen.
Management VLAN	This field displays the management VLAN ID if VLAN is active, or **Disabled** if it is not active. You can enable or disable VLAN, or change the management VLAN ID, in the **VLAN** > **Wireless VLAN** screen.
IP	This field displays the current IP address of the ZyXEL Device on the network.
LAN MAC	This displays the MAC (Media Access Control) address of the ZyXEL Device on the LAN. Every network device has a unique MAC address which identifies it across the network. Your ZyXEL Device features dual wireless module, and has two MAC addresses. The MAC address of the first wireless module (**WLAN1**) is used on the LAN.
WLAN1 MAC	This displays the MAC address of the first wireless module.
WLAN2 MAC	This displays the MAC address of the second wireless module.
System Resources	
Flash	This field displays the amount of the ZyXEL Device's flash memory currently in use. The flash memory is used to store firmware and SSID profiles.
Memory	This field displays what percentage of the ZyXEL Device's volatile memory is currently in use. The higher the memory usage, the more likely the ZyXEL Device is to slow down. Some memory is required just to start the ZyXEL Device and to run the web configurator.
CPU	This field displays what percentage of the ZyXEL Device's processing ability is currently being used. The higher the CPU usage, the more likely the ZyXEL Device is to slow down.
WLAN1 Associations	This field displays the number of wireless clients currently associated with the first wireless module. Each wireless module supports up to 128 concurrent associations.
WLAN2 Associations	This field displays the number of wireless clients currently associated with the second wireless module. Each wireless module supports up to 128 concurrent associations.
Interface Status	
Interface	This column displays each interface of the ZyXEL Device.

Table 1 The Status Screen

LABEL	DESCRIPTION
Status	This field indicates whether or not the ZyXEL Device is using the interface. For each interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface.
Rate	For the LAN port this displays the port speed and duplex setting. For the WLAN1 and WLAN2 interfaces, it displays the downstream and upstream transmission rate or **N/A** if the interface is not in use.
SSID Status	
Interface	This column displays each of the ZyXEL Device's wireless interfaces, **WLAN1** and **WLAN2**.
SSID	This field displays the SSID(s) currently used by each wireless module.
BSSID	This field displays the MAC address of the wireless adaptor.
Security	This field displays the type of wireless security used by each SSID.
VLAN	This field displays the VLAN ID of each SSID in use, or **Disabled** if the SSID does not use VLAN.
System Status	
Show Statistics	Click this link to view port status and packet specific statistics. See Section 18.2.1 on page 222.
Association List	Click this to see a list of wireless clients currently associated to each of the ZyXEL Device's wireless modules. See Section 18.3 on page 223.
Channel Usage	Click this to see which wireless channels are currently in use in the local area. See Section 18.4 on page 224.
Logs	Click this to see a list of logs produced by the ZyXEL Device. See Section 16.1 on page 195.
Rogue AP List	Click this to see a list of unauthorized access points in the local area. See Section 12.3.3 on page 149.

4

Management Mode

This chapter discusses the **MGNT MODE** (Management Mode) screen. This screen determines whether the ZyXEL Device is used in its default, standalone mode, or as part of a CAPWAP (Control And Provisioning of Wireless Access Points) network.

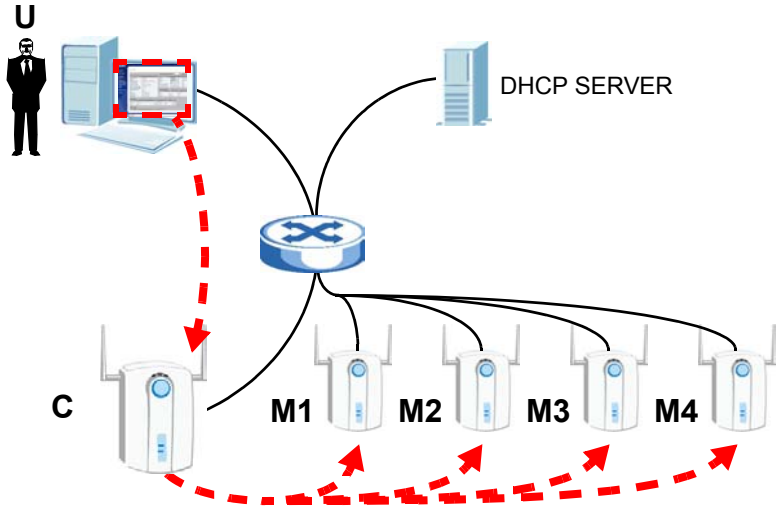
4.1 About CAPWAP

The ZyXEL Device supports CAPWAP (Control And Provisioning of Wireless Access Points). This is ZyXEL's implementation of the IETF's (Internet Engineering Task Force) CAPWAP protocol (RFC 4118).

The CAPWAP dataflow is protected by DTLS (Datagram Transport Layer Security).

The following figure illustrates a CAPWAP wireless network. You (**U**) configure the AP controller (**C**), which then automatically updates the configurations of the managed APs (**M1** ~ **M4**).

Figure 12 CAPWAP Network Example



The ZyXEL Device can be a standalone AP (default) or a CAPWAP managed AP. It cannot be a CAPWAP AP controller.

4.1.1 CAPWAP Discovery and Management

The link between CAPWAP-enabled access points proceeds as follows:

1. An AP in managed AP mode joins a wired network (receives a dynamic IP address).
2. The AP sends out a management request, looking for an AP in CAPWAP AP controller mode.
3. If there is an AP controller on the network, it receives the management request. If the AP controller is in **Manual** mode it adds the details of the AP to its **Unmanaged Access Points** list, and you decide which available APs to manage. If the AP is in **Always Accept** mode, it automatically adds the AP to its **Managed Access Points** list and provides the managed AP with default configuration information, as well as securely transmitting the DTLS (Datagram Transport Layer Security) pre-shared key. The managed AP is ready for association with wireless clients.

4.1.2 CAPWAP and DHCP

CAPWAP managed APs must be DHCP clients, supplied with an IP address by a DHCP server on your network.

Furthermore, the AP controller must have a static IP address; it cannot be a DHCP client.

4.1.3 CAPWAP and IP Subnets

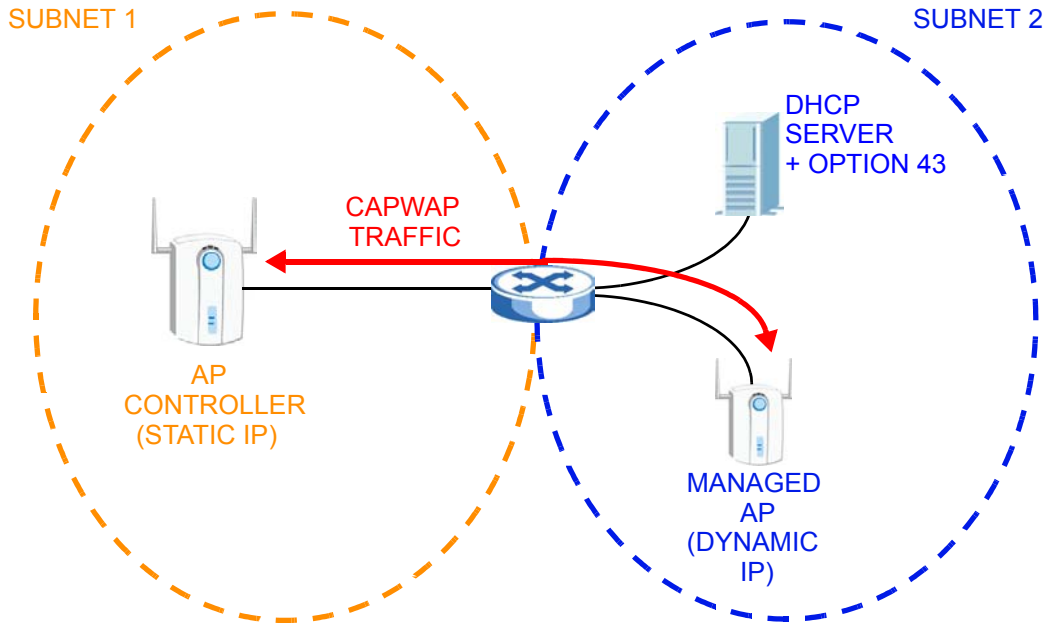
By default, CAPWAP works only between devices with IP addresses in the same subnet (see the appendices for information on IP addresses and subnetting).

However, you can configure CAPWAP to operate between devices with IP addresses in different subnets by doing the following.

- Activate DHCP option 43 on your network's DHCP server.
- Configure DHCP option 43 with the IP address of the CAPWAP AP controller on your network.

DHCP Option 43 allows the CAPWAP management request (from the AP in managed AP mode) to reach the AP controller in a different subnet, as shown in the following figure.

Figure 13 CAPWAP and DHCP Option 43



4.1.4 Notes on CAPWAP

This section lists some additional features of ZyXEL's implementation of the CAPWAP protocol.

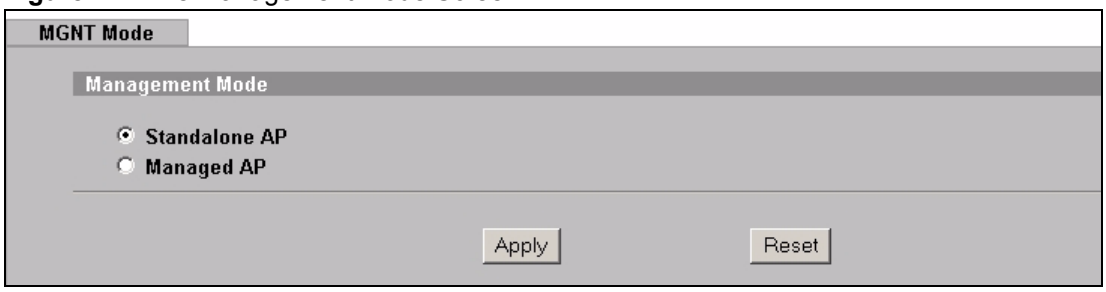
- When the AP controller uses its internal RADIUS server, managed APs also use the AP controller's authentication server to authenticate wireless clients.
- Only one AP controller can exist in any single broadcast domain.
- If a managed AP's link to the AP controller is broken, the managed AP continues to use the wireless settings with which it was last provided.

4.2 The Management Mode Screen

Use this screen to configure the ZyXEL Device as a CAPWAP managed AP, or to use it in its default standalone mode.

Click **MGNT MODE** in the ZyXEL Device's navigation menu. The following screen displays.

Figure 14 The Management Mode Screen



The following table describes the labels in this screen.

Table 2 The Management Mode Screen

LABEL	DESCRIPTION
Standalone AP	Select this to manage the ZyXEL Device using its own web configurator, neither managing nor managed by other devices.
Managed AP	Select this to have the ZyXEL Device managed by another ZyXEL Device on your network. When you do this, the ZyXEL Device can be configured ONLY by the management AP. If you do not have an AP controller on your network and want to return the ZyXEL Device to standalone mode, you must use its physical **RESET** button. All settings are returned to their default values. Note: When you set the ZyXEL Device to Managed AP mode, it becomes a DHCP client. To discover its new IP address, check the DHCP server on your network. If your network has no DHCP server, the ZyXEL Device's IP address remains the same. You can also check the **Controller** > **AP Lists** screen of the AP controller on your network.
Apply	Click this to save your changes. Note: If you change the mode in this screen, the ZyXEL Device restarts. Wait a short while before you attempt to log in again. If you changed the mode to **Managed AP**, you cannot log in as the web configurator is disabled; you must manage the ZyXEL Device through the management AP on your network.
Reset	Click this to return this screen to its previously-saved settings.

5

Tutorial

This chapter first provides an overview of how to configure the wireless LAN on your ZyXEL Device, and then gives step-by-step guidelines showing how to configure your ZyXEL Device for some example scenarios.

5.1 How to Configure the Wireless LAN

This section shows how to choose which wireless operating mode you should use on the ZyXEL Device, and the steps you should take to set up the wireless LAN in each wireless mode. See Section 5.1.3 on page 58 for links to more information on each step.

This section describes how to use the ZyXEL Device in standalone mode. For information on using the ZyXEL Device in a CAPWAP network, see Chapter 4 on page 51.

5.1.1 Choosing the Wireless Mode

- Use **Access Point** operating mode if you want to allow wireless clients to access your wired network, all using the same security and Quality of Service (QoS) settings. See Section 1.2.1 on page 34 for details.
- Use **Bridge/Repeater** operating mode if you want to use the ZyXEL Device to communicate with other access points. See Section 1.2.2 on page 34 for details.

  The ZyXEL Device is a bridge when other APs access your wired Ethernet network through the ZyXEL Device.

  The ZyXEL Device is a repeater when it has no Ethernet connection and allows other APs to communicate with one another through the ZyXEL Device.
- Use **AP+Bridge** operating mode if you want to use the ZyXEL Device as an access point (see above) while also communicating with other access points. See Section 1.2.3 on page 35 for details.
- Use **MBSSID** operating mode if you want to use the ZyXEL Device as an access point with some groups of users having different security or QoS settings from other groups of users. See Section 1.2.4 on page 36 for details.

5.1.1.1 Configuring Dual WLAN Adaptors

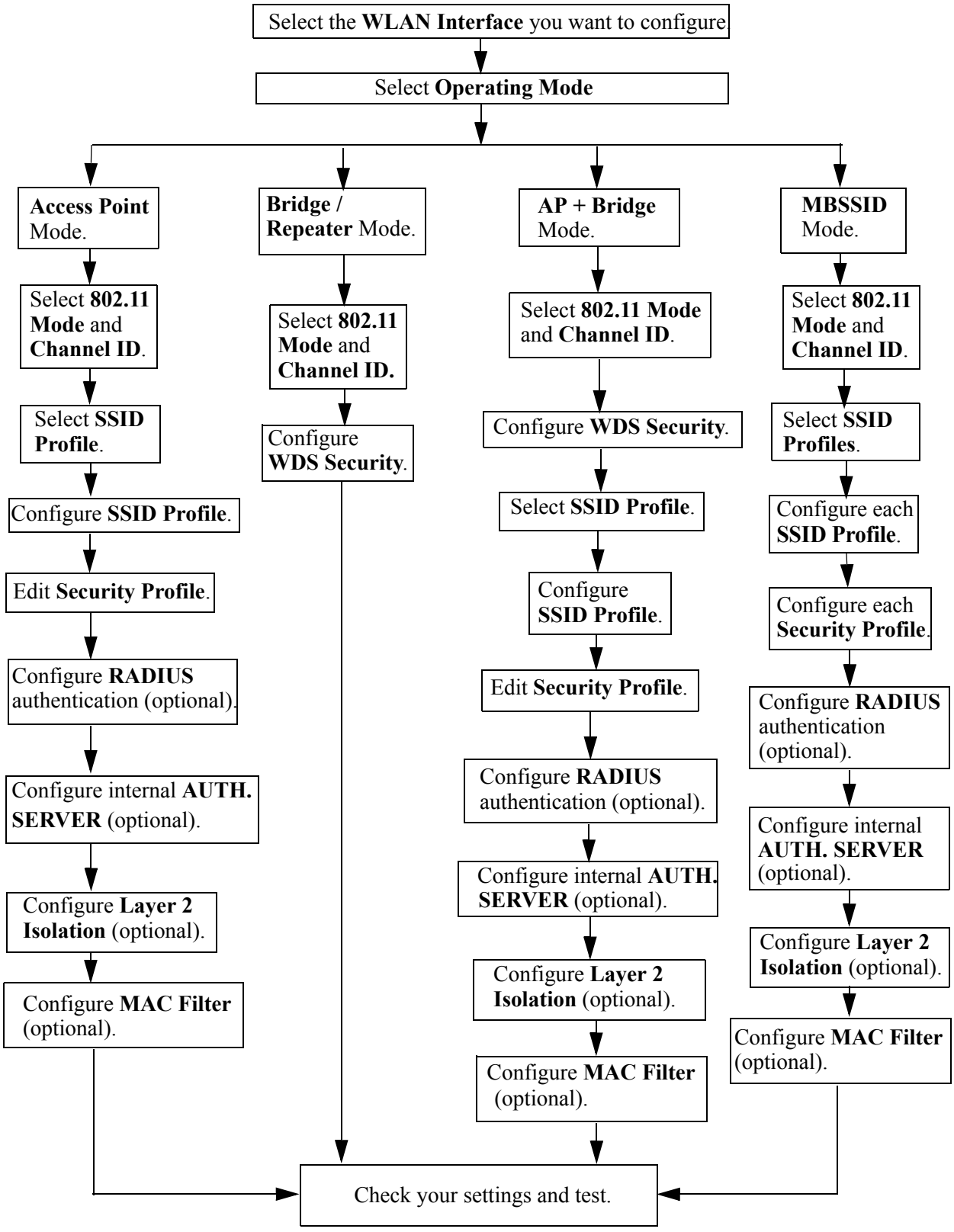
The ZyXEL Device is equipped with dual wireless adaptors. This means you can configure two different wireless networks to operate simultaneously. See Section 1.2.6 on page 37 for details.

You can configure each wireless adaptor separately in the **WIRELESS > Wireless** screen. To configure the first wireless network, select **WLAN1** in the **WLAN Interface** field and follow the steps in Section 5.1.2 on page 56. Then, select **WLAN2** in the **WLAN Interface** field and follow the same procedure to configure the second network.

5.1.2 Wireless LAN Configuration Overview

The following figure shows the steps you should take to configure the wireless settings according to the operating mode you select. Use the Web Configurator to set up your ZyXEL Device's wireless network (see your Quick Start Guide for information on setting up your ZyXEL Device and accessing the Web Configurator).

Figure 15 Configuring Wireless LAN



5.1.3 Further Reading

Use these links to find more information on the steps:

- Choosing **802.11 Mode**: see Section 7.7.1 on page 98.
- Choosing a wireless **Channel ID**: see Section 7.7.1 on page 98.
- Selecting and configuring **SSID profile**(s): see Section 7.7.1 on page 98 and Section 9.2.1 on page 125.
- Configuring and activating **WDS Security**: see Section 7.7.2 on page 101.
- Editing **Security Profile**(s): see Section 8.3 on page 111.
- Configuring an external **RADIUS** server: see Section 8.5 on page 119.
- Configuring and activating the internal **AUTH. SERVER**: see Section 8.4 on page 119 and Chapter 14 on page 169.
- Configuring **Layer 2 Isolation**: see Section 10.3 on page 131.
- Configuring **MAC Filtering**: see Section 10.4 on page 134.

5.2 How to Configure Multiple Wireless Networks

In this example, you have been using your ZyXEL Device as an access point for your office network (See your Quick Start Guide for information on how to set up your ZyXEL Device in Access Point mode). Now your network is expanding and you want to make use of the MBSSID feature (see Section 9.1 on page 121) to provide multiple wireless networks. Each wireless network will cater for a different type of user.

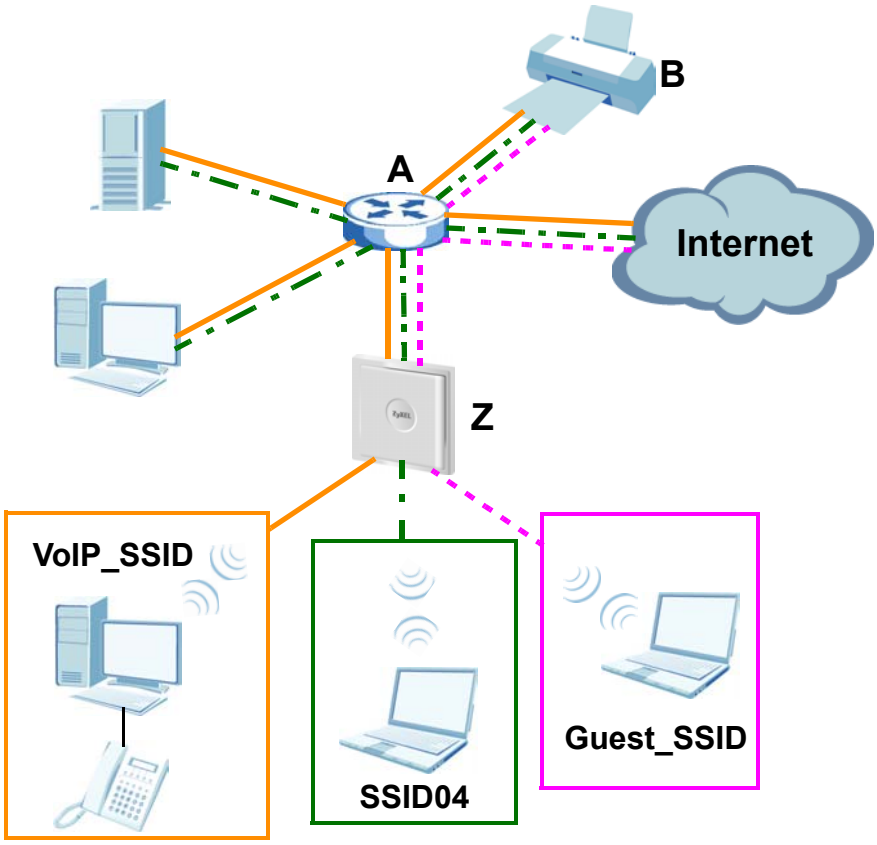
You want to make three wireless networks: one standard office wireless network with all the same settings you already have, another wireless network with high Quality of Service (QoS) settings for Voice over IP users, and a guest network that allows visitors to your office to access only the Internet and the network printer.

To do this, you will take the following steps:

1. Change the operating mode from Access Point to MBSSID and reactivate the standard network.
2. Configure a wireless network for Voice over IP users.
3. Configure a wireless network for guests to your office.

The following figure shows the multiple networks you want to set up. Your ZyXEL Device is marked **Z**, the main network router is marked **A**, and your network printer is marked **B**.

Figure 16 Tutorial: Example MBSSID Setup



The standard network (**SSID04**) has access to all resources. The VoIP network (**VoIP_SSID**) has access to all resources and a high Quality of Service (QoS) setting (see Chapter 7 on page 91 for information on QoS). The guest network (**Guest_SSID**) has access to the Internet and the network printer only, and a low QoS setting.

To configure these settings, you need to know the MAC (Media Access Control) addresses of the devices you want to allow users of the guest network to access. The following table shows the addresses used in this example.

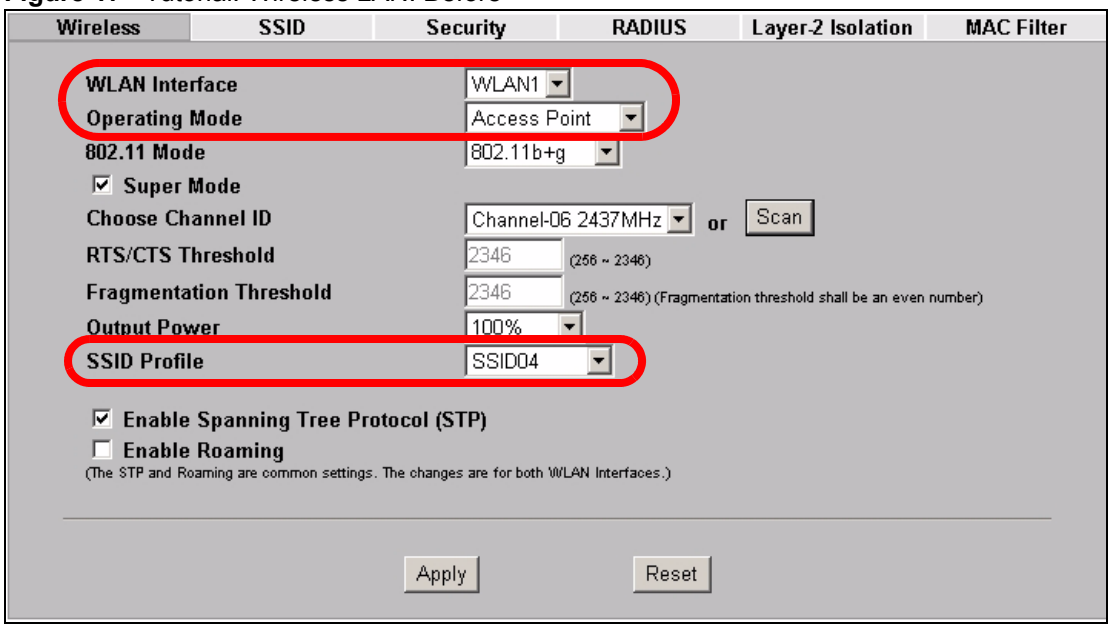
Table 3 Tutorial: Example Information

Network router (**A**) MAC address	00:AA:00:AA:00:AA
Network printer (**B**) MAC address	AA:00:AA:00:AA:00

5.2.1 Change the Operating Mode

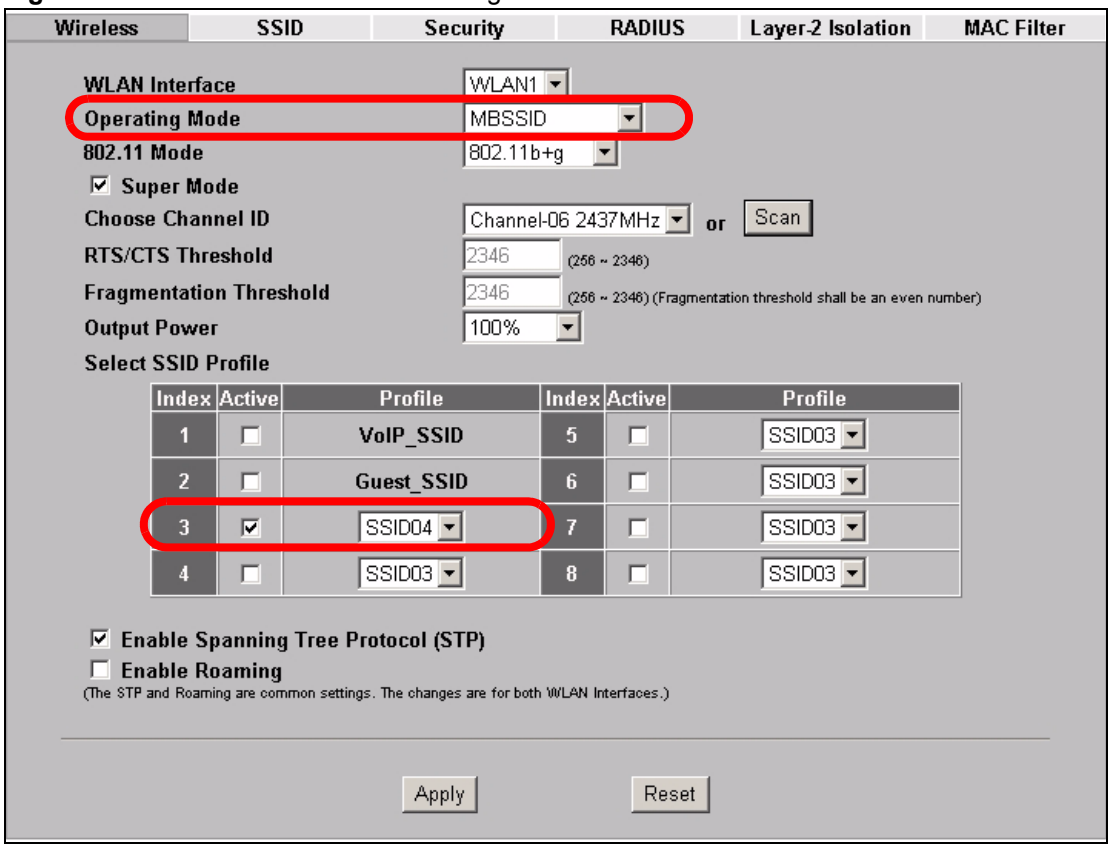
Log in to the ZyXEL Device (see Section 2.1 on page 43). Click **WIRELESS** > **Wireless**. The **Wireless** screen appears. In this example, the ZyXEL Device is using **WLAN Interface 1** in **Access Point** operating mode, and is currently set to use the **SSID04** profile.

Figure 17 Tutorial: Wireless LAN: Before



Select **MBSSID** from the **Operating Mode** drop-down list box. The screen displays as follows.

Figure 18 Tutorial: Wireless LAN: Change Mode



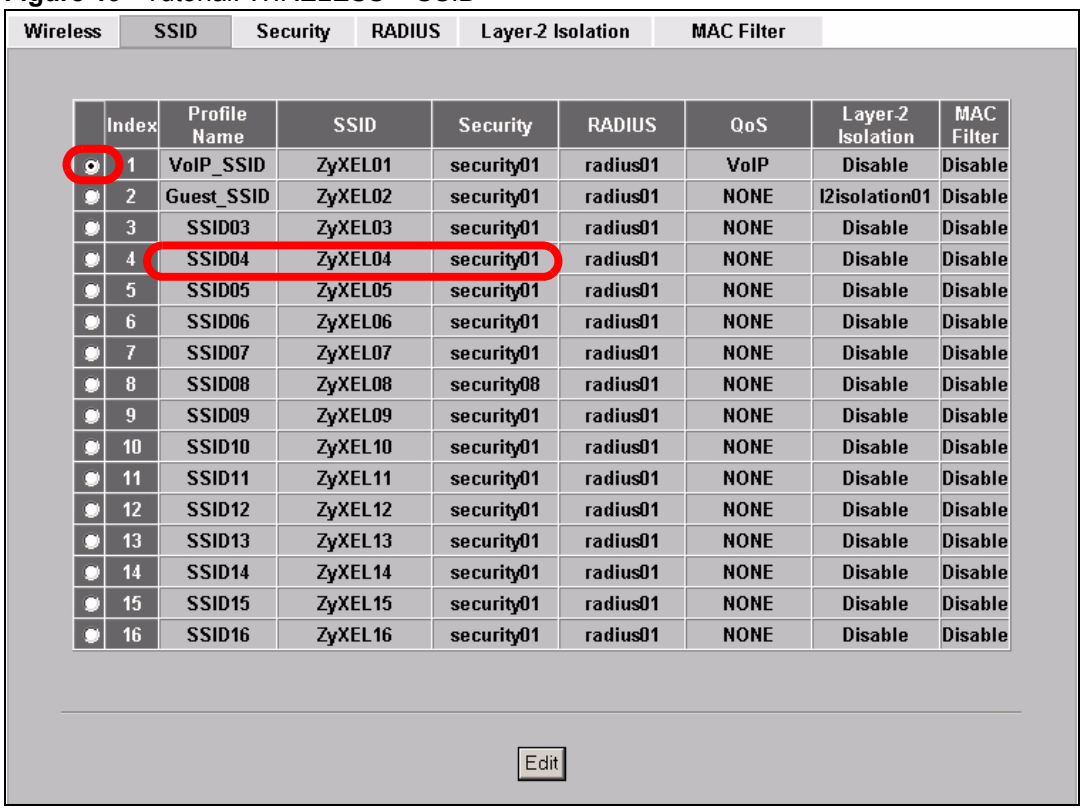
This **Select SSID Profile** table allows you to activate or deactivate SSID profiles. Your wireless network was previously using the **SSID04** profile, so select **SSID04** in one of the **Profile** list boxes (number **3** in this example).

Select the **Active** box for the entry and click **Apply** to activate the profile. Your standard wireless network (**SSID04**) is now accessible to your wireless clients as before. You do not need to configure anything else for your standard network.

5.2.2 Configure the VoIP Network

Next, click **WIRELESS** > **SSID**. The following screen displays. Note that the **SSID04** SSID profile (the standard network) is using the **security01** security profile. You cannot change this security profile without changing the standard network's parameters, so when you set up security for the **VoIP_SSID** and **Guest_SSID** profiles you will need to set different security profiles.

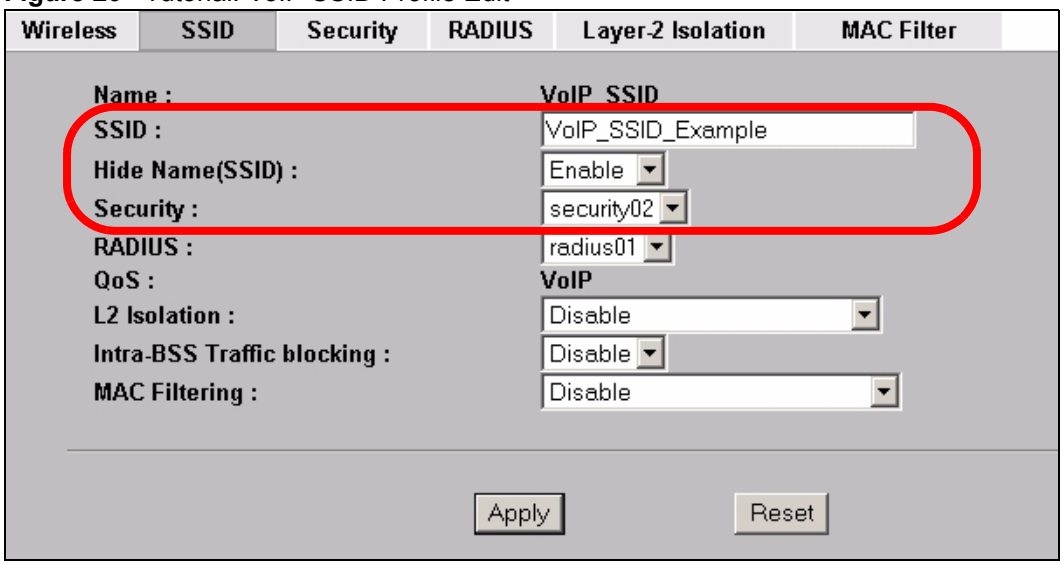
Figure 19 Tutorial: WIRELESS > SSID



	Index	Profile Name	SSID	Security	RADIUS	QoS	Layer-2 Isolation	MAC Filter
◉	1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
○	2	Guest_SSID	ZyXEL02	security01	radius01	NONE	l2isolation01	Disable
○	3	SSID03	ZyXEL03	security01	radius01	NONE	Disable	Disable
○	4	SSID04	ZyXEL04	security01	radius01	NONE	Disable	Disable
○	5	SSID05	ZyXEL05	security01	radius01	NONE	Disable	Disable
○	6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
○	7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable
○	8	SSID08	ZyXEL08	security08	radius01	NONE	Disable	Disable
○	9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable
○	10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable
○	11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable
○	12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable
○	13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable
○	14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable
○	15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable
○	16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable

The Voice over IP (VoIP) network will use the pre-configured SSID profile, so select **VoIP_SSID**'s radio button and click **Edit**. The following screen displays.

Figure 20 Tutorial: VoIP SSID Profile Edit

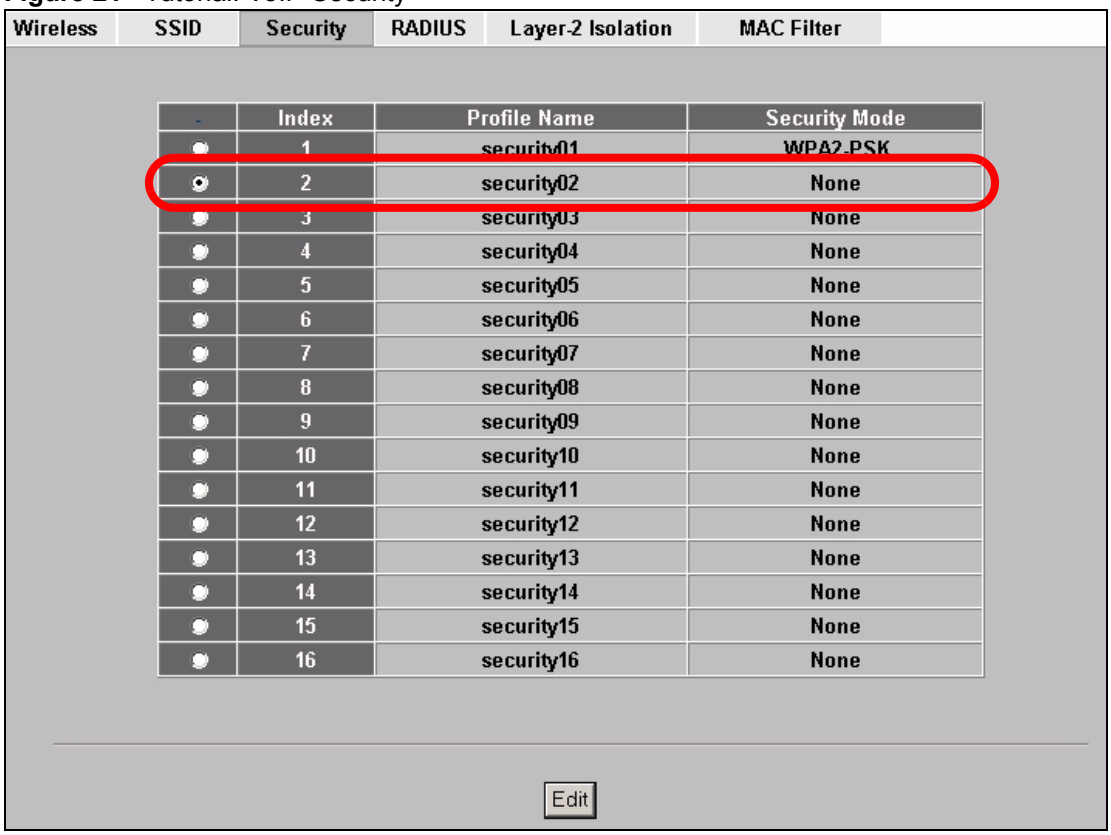


- Choose a new SSID for the VoIP network. In this example, enter **VOIP_SSID_Example**. Note that although the SSID changes, the SSID profile name (**VoIP_SSID**) remains the same as before.
- Select **Enable** from the **Hide Name (SSID)** list box. You want only authorized company employees to use this network, so there is no need to broadcast the SSID to wireless clients scanning the area.
- The standard network (**SSID04**) is currently using the **security01** profile, so use a different profile for the VoIP network. If you used the **security01** profile, anyone who could access the standard network could access the VoIP wireless network. Select **security02** from the **Security** field.
- Leave all the other fields at their defaults and click **Apply**.

5.2.2.1 Set Up Security for the VoIP Profile

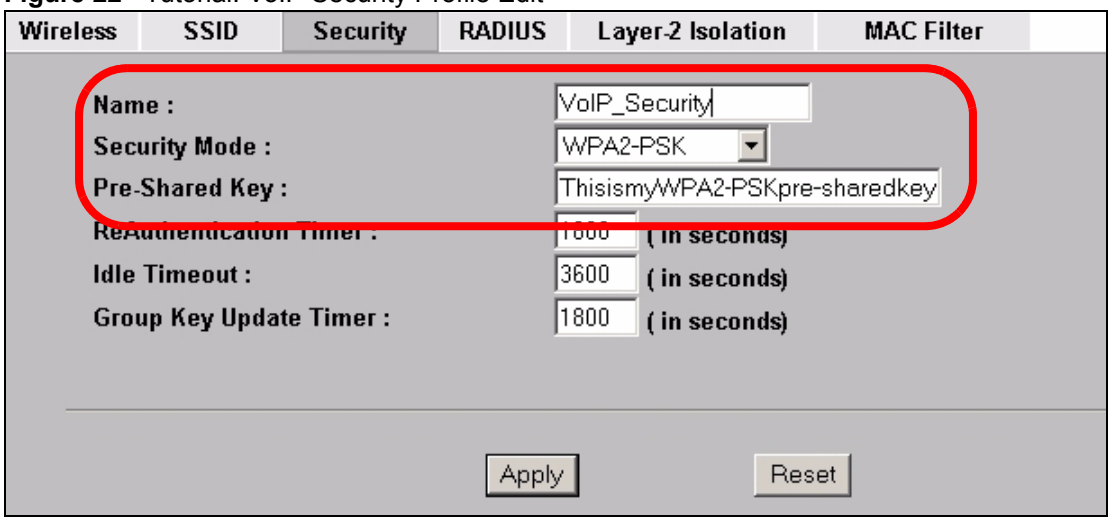
Now you need to configure the security settings to use on the VoIP wireless network. Click the **Security** tab.

Figure 21 Tutorial: VoIP Security



You already chose to use the **security02** profile for this network, so select the radio button for **security02** and click **Edit**. The following screen appears.

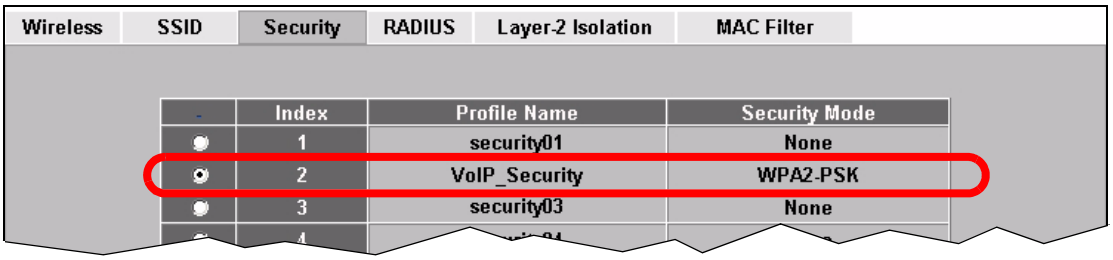
Figure 22 Tutorial: VoIP Security Profile Edit



- Change the **Name** field to "VoIP_Security" to make it easier to remember and identify.
- In this example, you do not have a RADIUS server for authentication, so select **WPA2-PSK** in the **Security Mode** field. WPA2-PSK provides strong security that anyone with a compatible wireless client can use, once they know the pre-shared key (PSK). Enter the PSK you want to use in your network in the **Pre-Shared Key** field. In this example, the PSK is "ThisismyWPA2-PSKpre-sharedkey".

- Click **Apply**. The **WIRELESS > Security** screen displays. Ensure that the **Profile Name** for entry 2 displays "**VoIP_Security**" and that the **Security Mode** is **WPA2-PSK**.

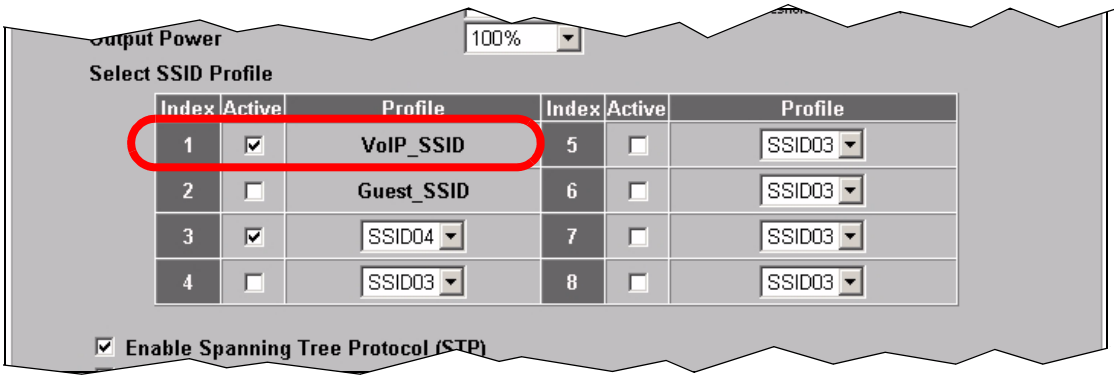
Figure 23 Tutorial: VoIP Security: Updated



5.2.2.2 Activate the VoIP Profile

You need to activate the **VoIP_SSID** profile before it can be used. Click the **Wireless** tab. In the **Select SSID Profile** table, select the **VoIP_SSID** profile's **Active** checkbox and click **Apply**.

Figure 24 Tutorial: Activate VoIP Profile



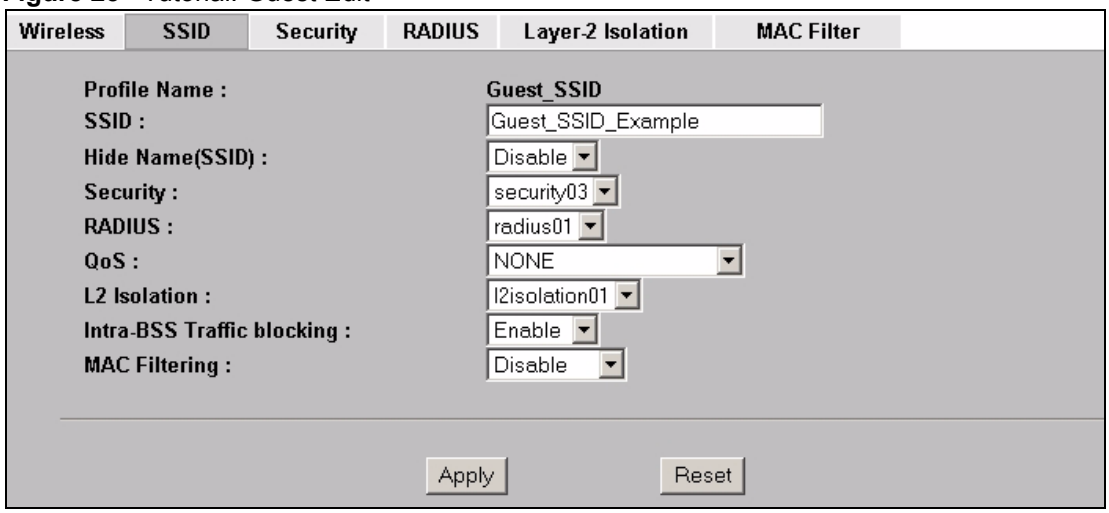
Your VoIP wireless network is now ready to use. Any traffic using the **VoIP_SSID** profile will be given the highest priority across the wireless network.

5.2.3 Configure the Guest Network

When you are setting up the wireless network for guests to your office, your primary concern is to keep your network secure while allowing access to certain resources (such as a network printer, or the Internet). For this reason, the pre-configured **Guest_SSID** profile has layer-2 isolation and intra-BSS traffic blocking enabled by default. "Layer-2 isolation" means that a client accessing the network via the **Guest_SSID** profile can access only certain pre-defined devices on the network (see Section 10.1 on page 129), and "intra-BSS traffic blocking" means that the client cannot access other clients on the same wireless network (see Section 9.2 on page 125).

Click **WIRELESS** > **SSID**. Select **Guest_SSID**'s entry in the list and click **Edit**. The following screen appears.

Figure 25 Tutorial: Guest Edit



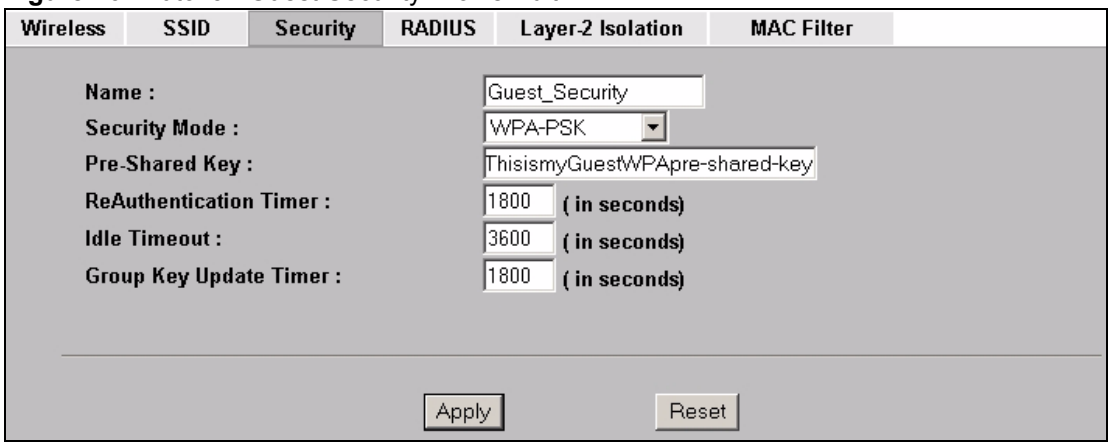
- Choose a new SSID for the guest network. In this example, enter **Guest_SSID_Example**. Note that although the SSID changes, the SSID profile name (**Guest_SSID**) remains the same as before.
- Select **Disable** from the **Hide Name (SSID)** list box. This makes it easier for guests to configure their own computers' wireless clients to your network's settings.
- The standard network (**SSID04**) is already using the **security01** profile, and the VoIP network is using the **security02** profile (renamed **VoIP_Security**) so select the **security03** profile from the **Security** field.
- Leave all the other fields at their defaults and click **Apply**.

5.2.3.1 Set Up Security for the Guest Profile

Now you need to configure the security settings to use on the guest wireless network. Click the **Security** tab.

You already chose to use the **security03** profile for this network, so select **security03**'s entry in the list and click **Edit**. The following screen appears.

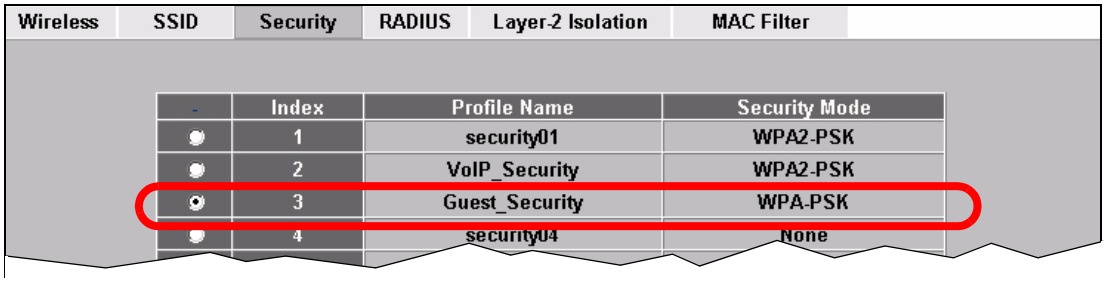
Figure 26 Tutorial: Guest Security Profile Edit



- Change the **Name** field to "Guest_Security" to make it easier to remember and identify.

- Select **WPA-PSK** in the **Security Mode** field. WPA-PSK provides strong security that is supported by most wireless clients. Even though your **Guest_SSID** clients do not have access to sensitive information on the network, you should not leave the network without security. An attacker could still cause damage to the network or intercept unsecured communications.
- Enter the PSK you want to use in your network in the **Pre-Shared Key** field. In this example, the PSK is "ThisismyGuestWPApre-sharedkey".
- Click **Apply**. The **WIRELESS > Security** screen displays. Ensure that the **Profile Name** for entry 3 displays "**Guest_Security**" and that the **Security Mode** is **WPA-PSK**.

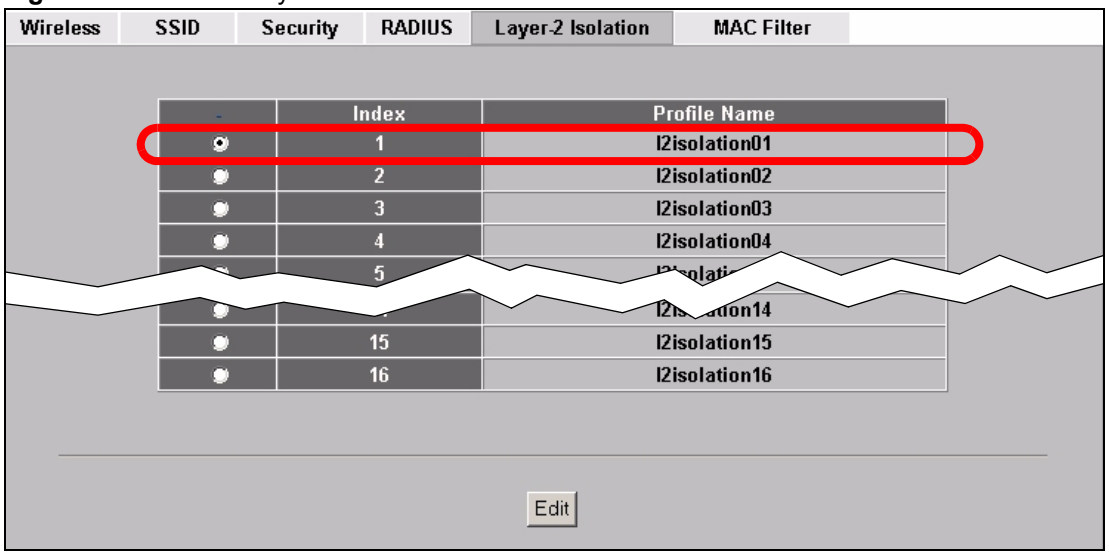
Figure 27 Tutorial: Guest Security: Updated



5.2.3.2 Set up Layer 2 Isolation

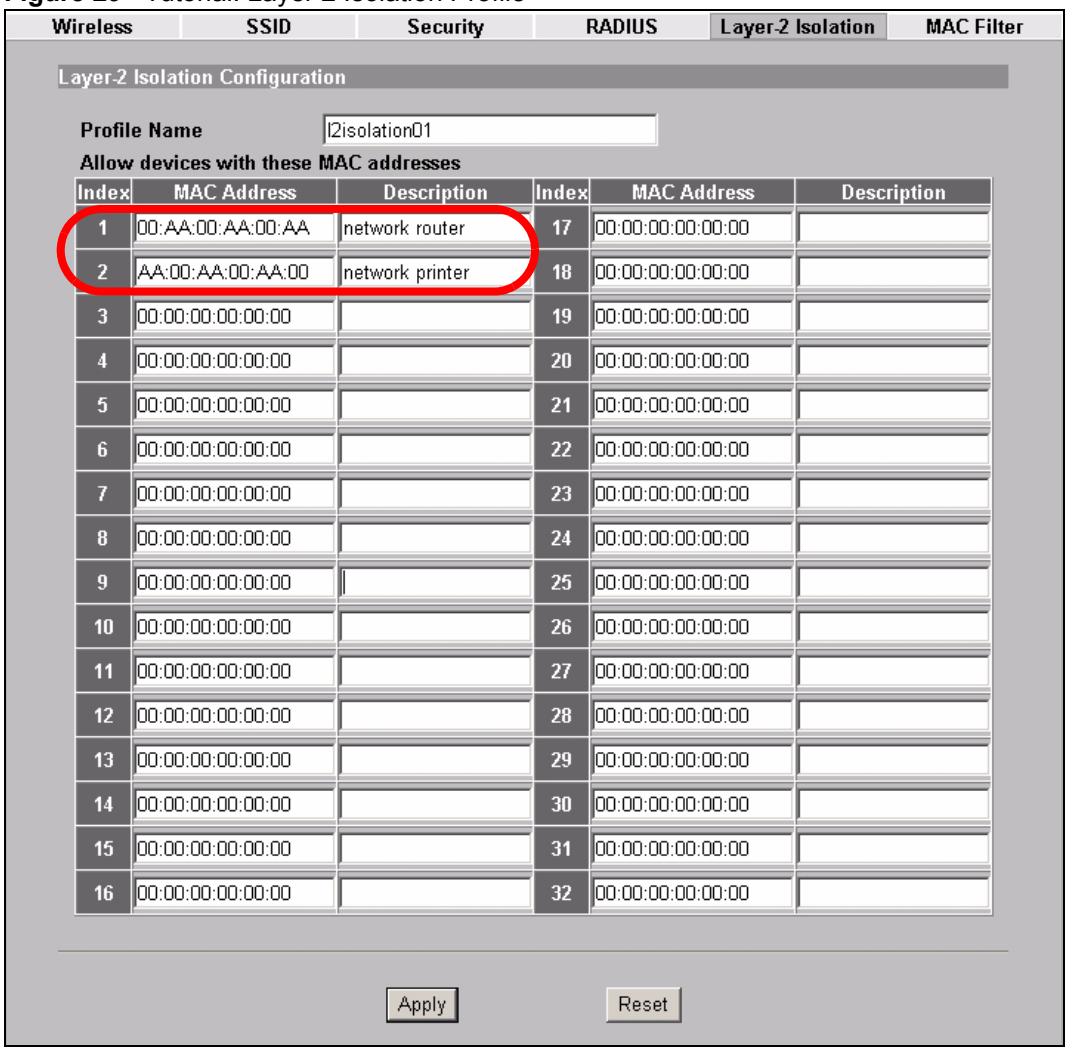
Configure layer 2 isolation to control the specific devices you want the users on your guest network to access. Click **WIRELESS** > **Layer-2 Isolation**. The following screen appears.

Figure 28 Tutorial: Layer 2 Isolation



The **Guest_SSID** network uses the **l2isolation01** profile by default, so select its entry and click **Edit**. The following screen displays.

Figure 29 Tutorial: Layer 2 Isolation Profile

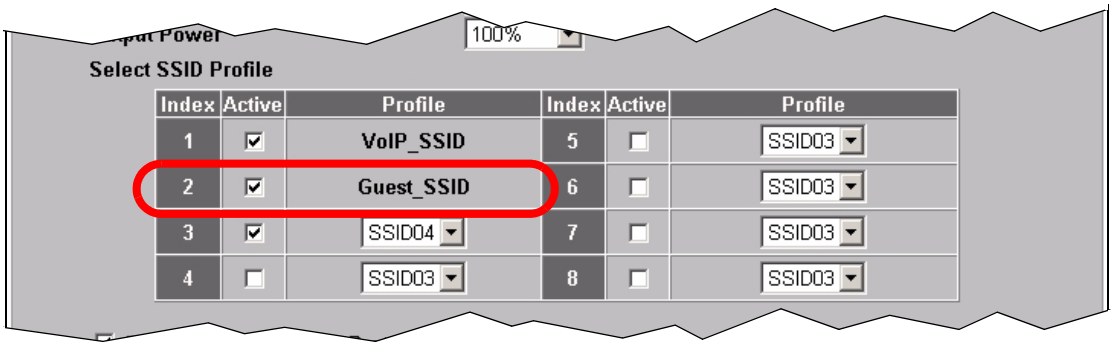


Enter the MAC addresses and descriptions of the two network devices you want users on the guest network to be able to access: the main network router (00:AA:00:AA:00:AA) and the network printer (AA:00:AA:00:AA:00). Click **Apply**.

5.2.3.3 Activate the Guest Profile

You need to activate the **Guest_SSID** profile before it can be used. Click the **Wireless** tab. In the **Select SSID Profile** table, select the check box for the **Guest_SSID** profile and click **Apply**.

Figure 30 Tutorial: Activate Guest Profile



Your guest wireless network is now ready to use.

5.2.4 Testing the Wireless Networks

To make sure that the three networks are correctly configured, do the following.

- On a computer with a wireless client, scan for access points. You should see the **Guest_SSID** network, but not the **VoIP_SSID** network. If you can see the **VoIP_SSID** network, go to its **SSID Edit** screen and make sure **Hide Name (SSID)** is set to **Enable**.

  Whether or not you see the standard network's SSID (**SSID04**) depends on whether "hide SSID" is enabled.
- Try to access each network using the correct security settings, and then using incorrect security settings, such as the WPA-PSK for another active network. If the behavior is different from expected (for example, if you can access the VoIP wireless network using the security settings for the **Guest_SSID** wireless network) check that the SSID profile is set to use the correct security profile, and that the settings of the security profile are correct.
- Access the **Guest_SSID** network and try to access other resources than those specified in the Layer 2 Isolation (**l2isolation01**) profile screen.

  You can use the ping utility to do this. Click **Start** > **Run...** and enter "cmd" in the **Open:** field. Click **OK**. At the **c:\>** prompt, enter "ping 192.168.1.10" (substitute the IP address of a real device on your network that is not on the layer 2 isolation list). If you receive a reply, check the settings in the **WIRELESS** > **Layer-2 Isolation > Edit** screen, and ensure that the correct layer 2 isolation profile is enabled in the **Guest_SSID** profile screen.

5.3 How to Set Up and Use Rogue AP Detection

This example shows you how to configure the rogue AP detection feature on the ZyXEL Device.

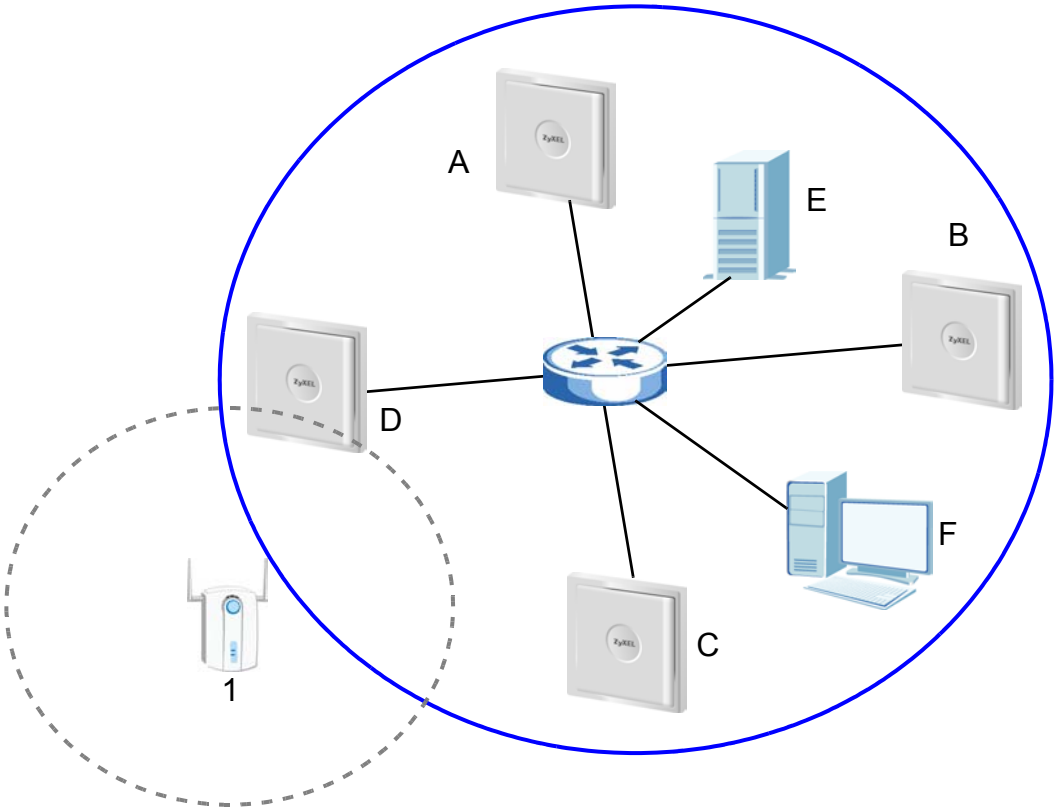
A rogue AP is a wireless access point operating in a network's coverage area that is not a sanctioned part of that network. The example also shows how to set the ZyXEL Device to send out e-mail alerts whenever it detects a rogue wireless access point. See Chapter 12 on page 145 for background information on the rogue AP function and security considerations.

In this example, you want to ensure that your company's data is not accessible to an attacker gaining entry to your wireless network through a rogue AP.

Your wireless network operates in an office building. It consists of four access points (all ZyXEL Devices) and a variable number of wireless clients. You also know that the coffee shop on the ground floor has a wireless network consisting of a single access point, which can be detected and accessed from your floor of the building. There are no other static wireless networks in your coverage area.

The following diagram shows the wireless networks in your area. Your access points are marked **A**, **B**, **C** and **D**. You also have a network mail/file server, marked **E**, and a computer, marked **F**, connected to the wired network. The coffee shop's access point is marked **1**.

Figure 31 Tutorial: Wireless Network Example



In the figure, the solid circle represents the range of your wireless network, and the dashed circle represents the extent of the coffee shop's wireless network. Note that the two networks overlap. This means that one or more of your APs can detect the AP (**1**) in the other wireless network.

When configuring the rogue AP feature on your ZyXEL Devices in this example, you will need to use the information in the following table. You need the IP addresses of your APs to access their Web configurators, and you need the MAC address of each AP to configure the friendly AP list. You need the IP address of the mail server to set up e-mail alerts.

Table 4 Tutorial: Rogue AP Example Information

DEVICE	IP ADDRESS	MAC ADDRESS
Access Point **A**	192.168.1.1	00:AA:00:AA:00:AA
Access Point **B**	192.168.1.2	AA:00:AA:00:AA:00
Access Point **C**	192.168.1.3	A0:0A:A0:0A:A0:0A

Table 4 Tutorial: Rogue AP Example Information

DEVICE	IP ADDRESS	MAC ADDRESS
Access Point **D**	192.168.1.4	0A:A0:0A:A0:0A:A0
File / Mail Server **E**	192.168.1.25	N/A
Access Point **1**	UNKNOWN	AF:AF:AF:FA:FA:FA

The ZyXEL Device can detect the MAC addresses of APs automatically. However, it is more secure to obtain the correct MAC addresses from another source and add them to the friendly AP list manually. For example, an attacker's AP mimicking the correct SSID could be placed on the friendly AP list by accident, if selected from the list of auto-detected APs. In this example you have spoken to the coffee shop's owner, who has told you the correct MAC address of his AP.

In this example, you will do the following things.

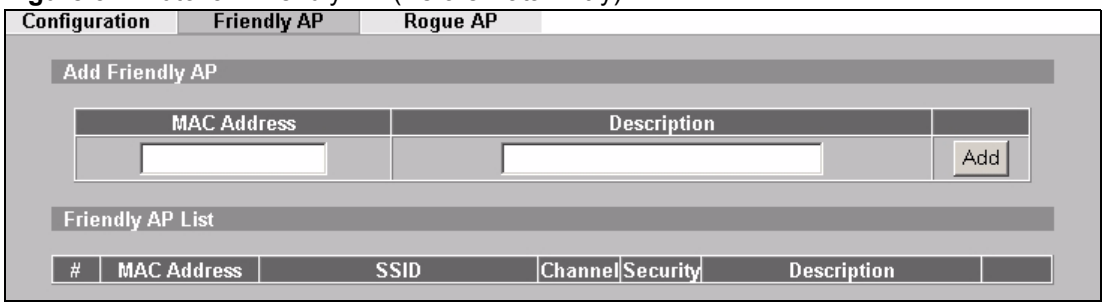
1. Set up and save a friendly AP list.
2. Activate periodic Rogue AP Detection.
3. Set up e-mail alerts.
4. Configure your other access points.
5. Test the setup.

5.3.1 Set Up and Save a Friendly AP list

Take the following steps to set up and save a list of access points you want to allow in your network's coverage area.

1. On a computer connected to the wired network (**F** in the previous figure), open your Internet browser and enter the URL of access point **A** (192.168.1.1). Login to the Web configurator and click **ROGUE AP** > **Friendly AP**. The following screen displays.

Figure 32 Tutorial: Friendly AP (Before Data Entry)



2 Fill in the **MAC Address** and **Description** fields as in the following table. Click **Add** after you enter the details of each AP to include it in the list.

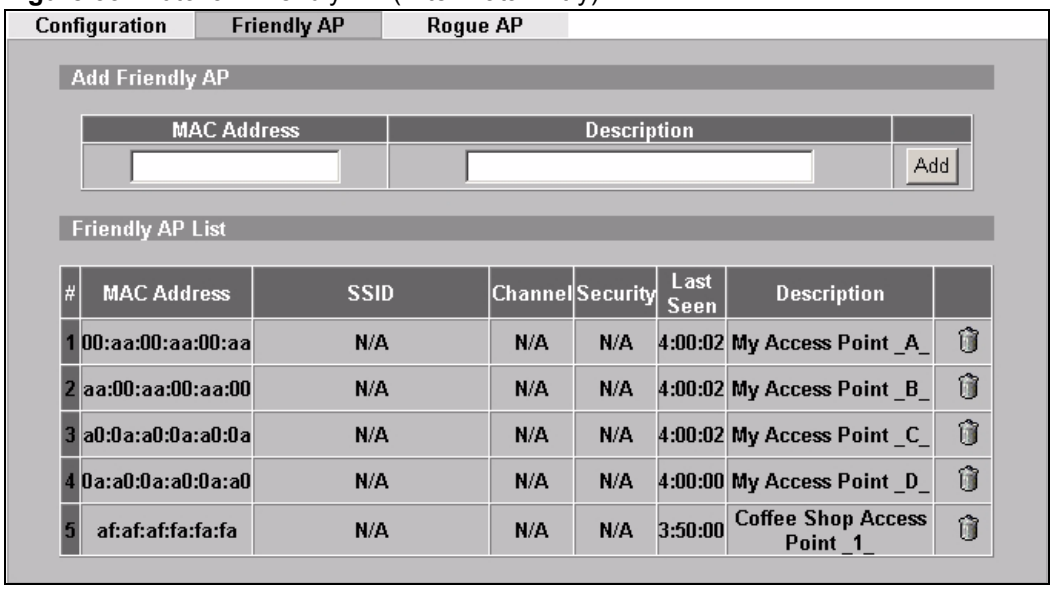
Table 5 Tutorial: Friendly AP Information

MAC ADDRESS	DESCRIPTION
00:AA:00:AA:00:AA	My Access Point _A_
AA:00:AA:00:AA:00	My Access Point _B_
A0:0A:A0:0A:A0:0A	My Access Point _C_
0A:A0:0A:A0:0A:A0	My Access Point _D_
AF:AF:AF:FA:FA:FA	Coffee Shop Access Point _1_

You can add APs that are not part of your network to the friendly AP list, as long as you know that they do not pose a threat to your network's security.

The **Friendly AP** screen now appears as follows.

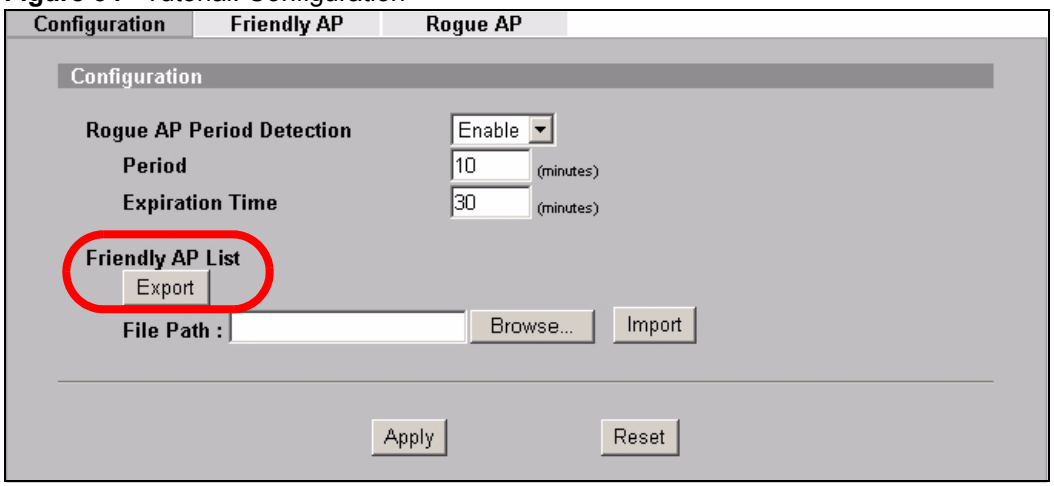
Figure 33 Tutorial: Friendly AP (After Data Entry)



3 Next, you will save the list of friendly APs in order to provide a backup and upload it to your other access points.

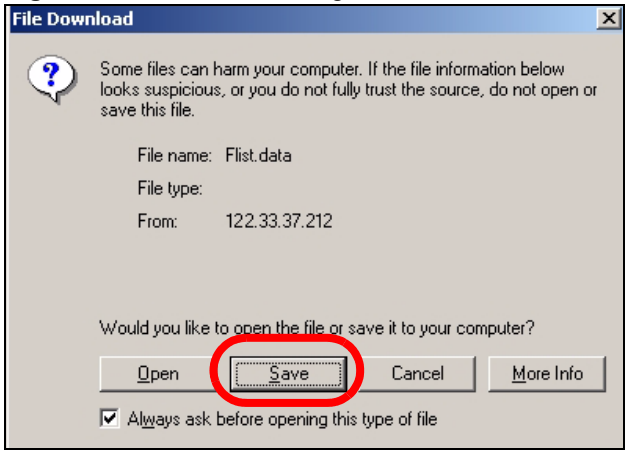
Click the **Configuration** tab.The following screen appears.

Figure 34 Tutorial: Configuration



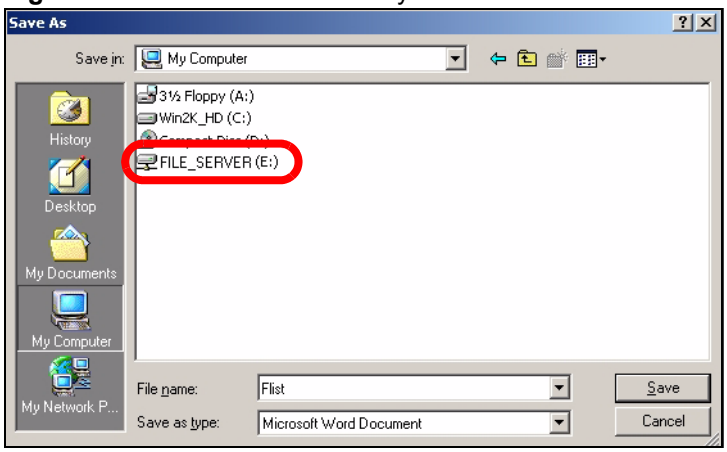
4 Click **Export**. If a window similar to the following appears, click **Save**.

Figure 35 Tutorial: Warning



5 Save the friendly AP list somewhere it can be accessed by all the other access points on the network. In this example, save it on the network file server (**E** in Figure 31 on page 69). The default filename is “Flist”.

Figure 36 Tutorial: Save Friendly AP list

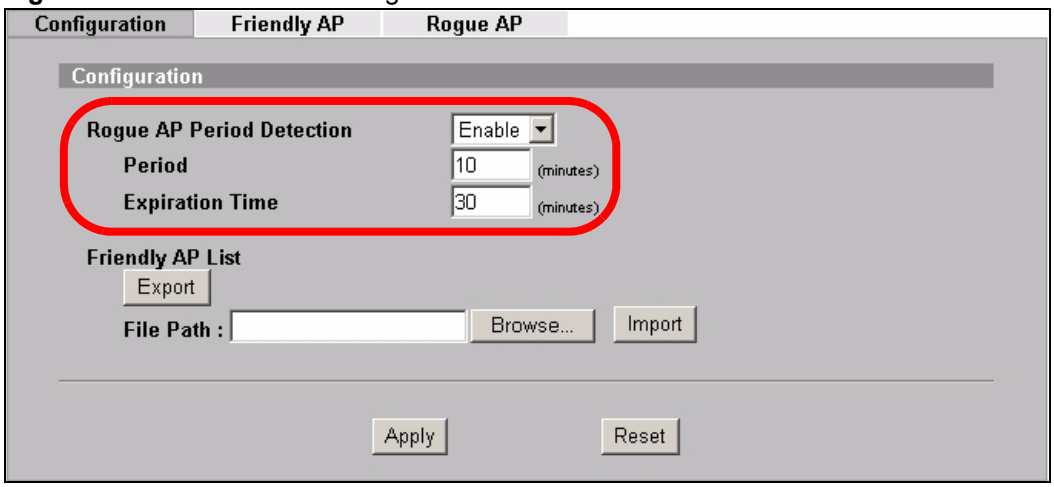


5.3.2 Activate Periodic Rogue AP Detection

Take the following steps to activate rogue AP detection on the first of your ZyXEL Devices.

1 In the **ROGUE AP** > **Configuration** screen, select **Enable** from the **Rogue AP Period Detection** field.

Figure 37 Tutorial: Periodic Rogue AP Detection



2 In the **Period** field, enter how often you want the ZyXEL Device to scan for rogue APs. You can have the ZyXEL Device scan anywhere from once every ten minutes to once every hour. In this example, enter "10".

3 In the **Expiration Time** field, enter how long an AP's entry can remain in the list before the ZyXEL Device discards it from the list when the AP is no longer active. In this example, enter "30".

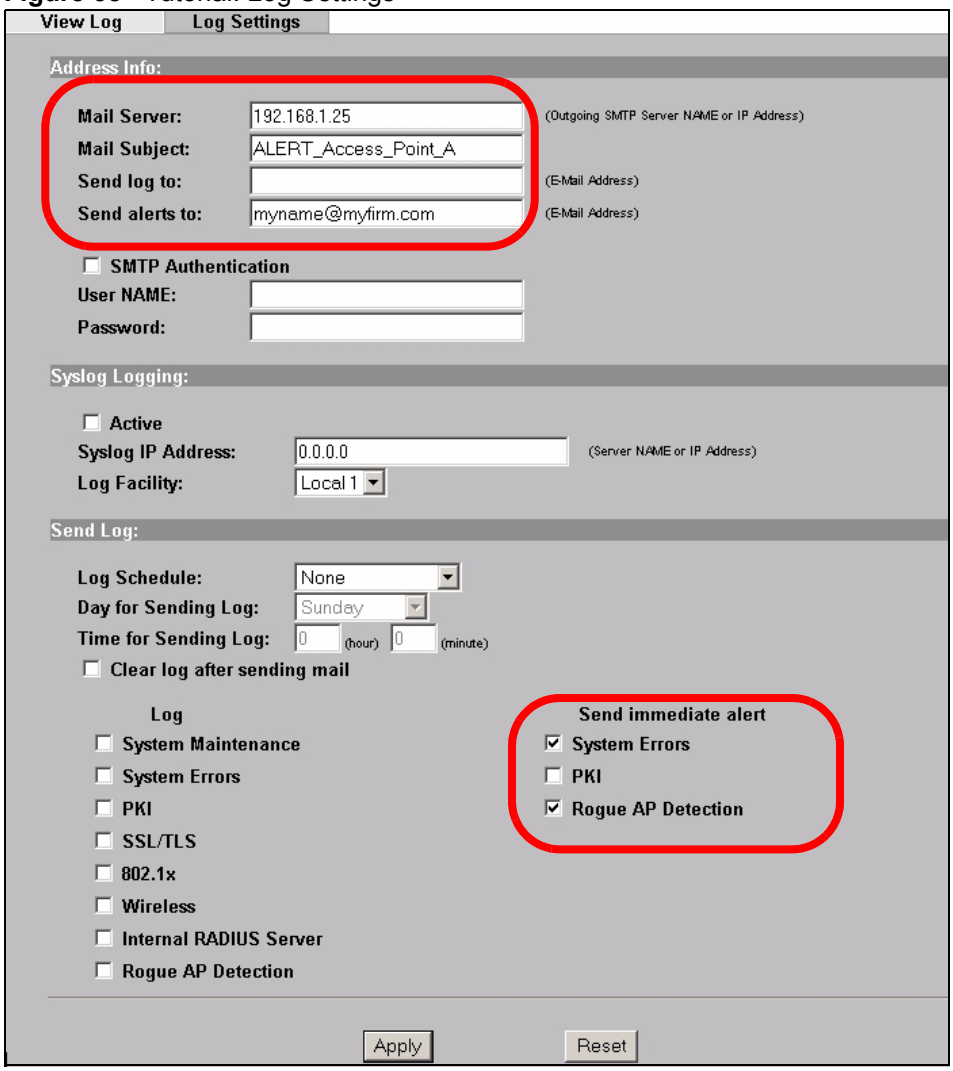
4 Click **Apply**.

5.3.3 Set Up E-mail Logs

In this section, you will configure the first of your four APs to send a log message to your e-mail inbox whenever a rogue AP is discovered in your wireless network's coverage area.

1 Click **LOGS** > **Log Settings**. The following screen appears.

Figure 38 Tutorial: Log Settings



- In this example, your mail server's IP address is **192.168.1.25**. Enter this IP address in the **Mail Server** field.
- Enter a subject line for the alert e-mails in the **Mail Subject** field. Choose a subject that is eye-catching and identifies the access point - in this example, "ALERT_Access_Point_A".
- Enter the email address to which you want alerts to be sent (**myname@myfirm.com**, in this example).
- In the **Send Immediate Alert** section, select the events you want to trigger immediate e-mails. Ensure that **Rogue AP Detection** is selected.
- Click **Apply**.

5.3.4 Configure Your Other Access Points

Access point **A** is now configured to do the following.

- Scan for access points in its coverage area every ten minutes.
- Recognize friendly access points from a list.
- Send immediate alerts to your email account if it detects an access point not on the list.

Now you need to configure the other wireless access points on your network to do the same things.

For each access point, take the following steps.

1. From a computer on the wired network, enter the access point's IP address and login to its Web configurator. See Table 4 on page 69 for the example IP addresses.
2. Import the friendly AP list. Click **ROGUE AP** > **Configuration** > **Browse...**. Find the "Flist" file where you previously saved it on the network and click **Open**.
3. Click **Import**. Check the **ROGUE AP** > **Friendly AP** screen to ensure that the friendly AP list has been correctly uploaded.
4. Activate periodic rogue AP detection. See Section 5.3.2 on page 73.
5. Set up e-mail logs as in Section 5.3.3 on page 73, but change the **Mail Subject** field so you can tell which AP the alerts come from ("ALERT_Access_Point_B", etc.)

5.3.5 Test the Setup

Next, test your setup to ensure it is correctly configured.

- Log into each AP's Web configurator and click **ROGUE AP** > **Rogue AP**. Click **Refresh**. If any of the MAC addresses from Table 5 on page 71 appear in the list, the friendly AP function may be incorrectly configured - check the **ROGUE AP** > **Friendly AP** screen.

  If any entries appear in the rogue AP list that are not in Table 5 on page 71, write down the AP's MAC address for future reference and check your e-mail inbox. If you have received a rogue AP alert, email alerts are correctly configured on that ZyXEL Device.
- If you have another access point that is not used in your network, make a note of its MAC address and set it up next to each of your ZyXEL Devices in turn while the network is running.

  Either wait for at least ten minutes (to ensure the ZyXEL Device performs a scan in that time) or login to the ZyXEL Device's Web configurator and click **ROGUE AP** > **Rogue AP** > **Refresh** to have the ZyXEL Device perform a scan immediately.
  - Check the **ROGUE AP** > **Rogue AP** screen. You should see an entry in the list with the same MAC address as your "rogue" AP.
  - Check the **LOGS** > **View Logs** screen. You should see a **Rogue AP Detection** entry in red text, including the MAC address of your "rogue" AP.
  - Check your e-mail. You should have received at least one e-mail alert (your other ZyXEL Devices may also have sent alerts, depending on their proximity and the output power of your "rogue" AP).

5.4 Using Multiple MAC Filters and L-2 Isolation Profiles

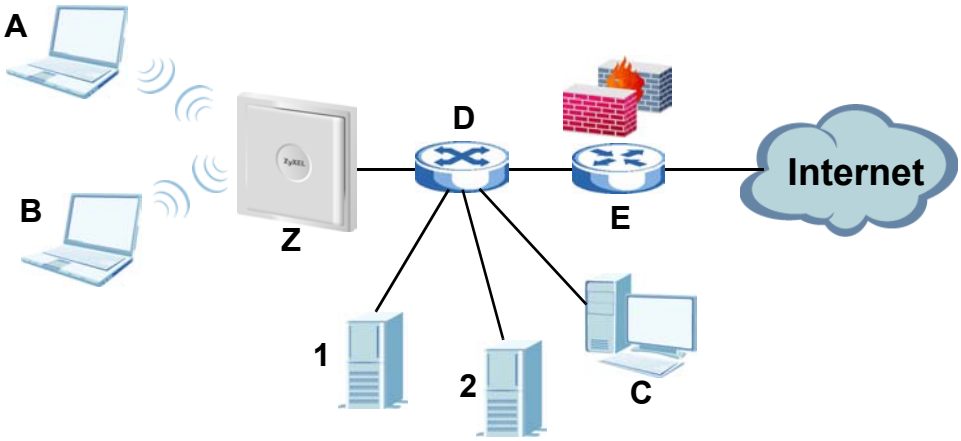
This example shows you how to allow certain users to access only specific parts of your network. You can do this by using multiple MAC filters and layer-2 isolation profiles.

5.4.1 Scenario

In this example, you run a company network in which certain employees must wirelessly access secure file servers containing valuable proprietary data.

You have two secure servers (**1** and **2** in the following figure). Wireless user "Alice" (**A**) needs to access server **1** (but should not access server **2**) and wireless user "Bob" (**B**) needs to access server **2** (but should not access server **1**). Your ZyXEL Device is marked **Z**. **C** is a workstation on your wired network, **D** is your main network switch, and **E** is the security gateway you use to connect to the Internet.

Figure 39 Tutorial: Example Network



5.4.2 Your Requirements

1. You want to set up a wireless network to allow only Alice to access Server **1** and the Internet.
2. You want to set up a second wireless network to allow only Bob to access Server **2** and the Internet.

5.4.3 Setup

In this example, you have already set up the ZyXEL Device in MBSSID mode (see Chapter 9 on page 121). It uses two SSID profiles simultaneously. You have configured each SSID profile as shown in the following table.

Table 6 Tutorial: SSID Profile Security Settings

SSID Profile Name	**SERVER_1**	**SERVER_2**
SSID	**SSID_S1**	**SSID_S2**
Security	Security Profile **security03**: WPA2-PSK Hide SSID	Security Profile **security04**: WPA2-PSK Hide SSID
Intra-BSS traffic blocking	Enabled	Enabled

Each SSID profile already uses a different pre-shared key.

In this example, you will configure access limitations for each SSID profile. To do this, you will take the following steps.

1. Configure the **SERVER_1** network's SSID profile to use specific MAC filter and layer-2 isolation profiles.

2 Configure the **SERVER_1** network's MAC filter profile.
3 Configure the **SERVER_1** network's layer-2 isolation profile.
4 Repeat steps 1 ~ 3 for the **SERVER_2** network.
5 Check your settings and test the configuration.

To configure layer-2 isolation, you need to know the MAC addresses of the devices on your network, which are as follows.

Table 7 Tutorial: Example Network MAC Addresses

DEVICE	LABEL	MAC ADDRESS
ZyXEL Device	Z	BB:AA:99:88:77:66
Secure Server 1	1	AA:99:88:77:66:55
Secure Server 2	2	99:88:77:66:55:44
Workstation	C	88:77:66:55:44:33
Switch	D	77:66:55:44:33:22
Security gateway	E	66:55:44:33:22:11

To configure MAC filtering, you need to know the MAC addresses of the devices Alice and Bob use to connect to the network, which are as follows.

Table 8 Tutorial: Example User MAC Addresses

USER	MAC ADDRESS
Alice	11:22:33:44:55:66
Bob	22:33:44:55:66:77

5.4.4 Configure the SERVER_1 Network

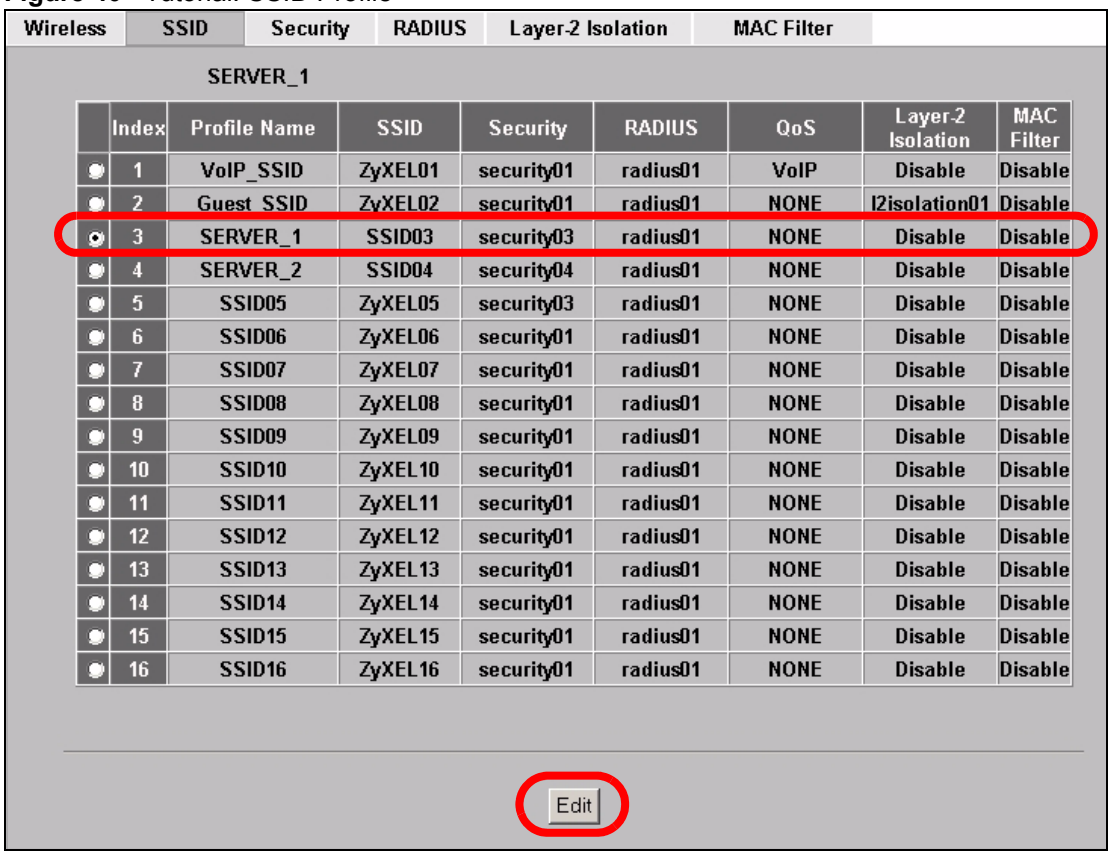
First, you will set up the **SERVER_1** network which allows Alice to access secure server **1** via the network switch.

You will configure the MAC filter to restrict access to Alice alone, and then configure layer-2 isolation to allow her to access only the network switch, the file server and the Internet security gateway.

Take the following steps to configure the **SERVER_1** network.

1 Log into the ZyXEL Device's Web Configurator and click **WIRELESS > SSID**. The following screen displays, showing the SSID profiles you already configured.

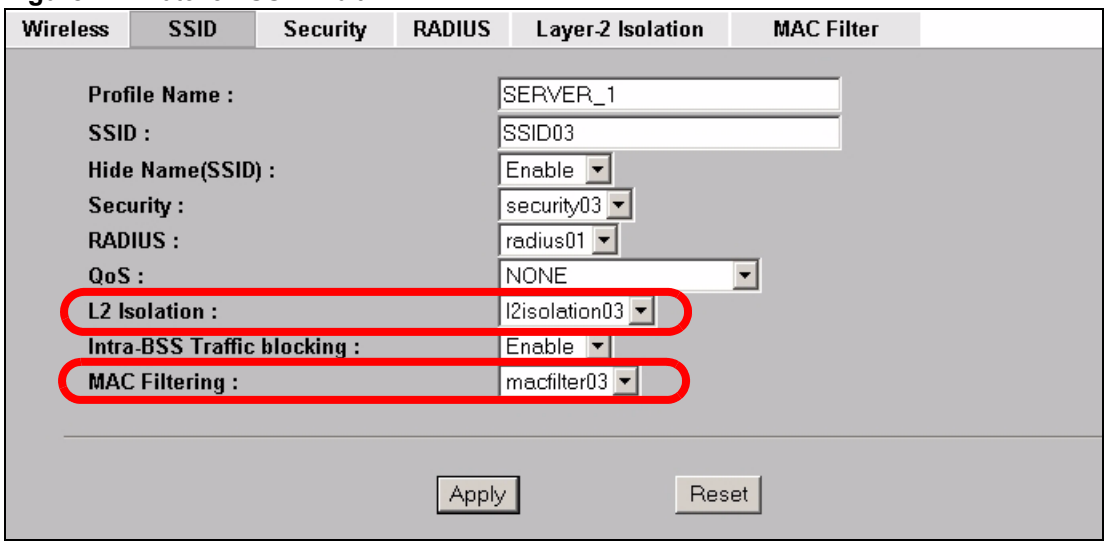
Figure 40 Tutorial: SSID Profile



	Index	Profile Name	SSID	Security	RADIUS	QoS	Layer-2 Isolation	MAC Filter
○	1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
○	2	Guest_SSID	ZyXEL02	security01	radius01	NONE	l2isolation01	Disable
◉	3	SERVER_1	SSID03	security03	radius01	NONE	Disable	Disable
○	4	SERVER_2	SSID04	security04	radius01	NONE	Disable	Disable
○	5	SSID05	ZyXEL05	security03	radius01	NONE	Disable	Disable
○	6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
○	7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable
○	8	SSID08	ZyXEL08	security01	radius01	NONE	Disable	Disable
○	9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable
○	10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable
○	11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable
○	12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable
○	13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable
○	14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable
○	15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable
○	16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable

2 Select **SERVER_1**'s entry and click **Edit**. The following screen displays.

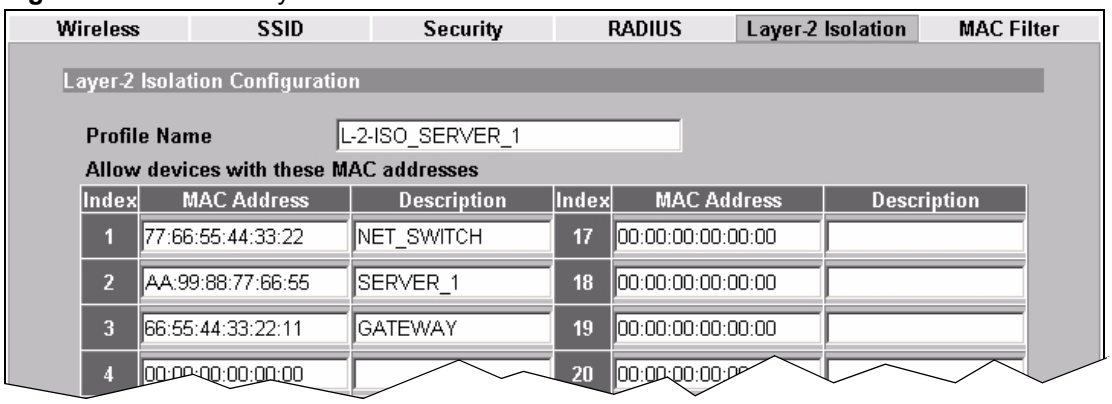
Figure 41 Tutorial: SSID Edit



Select **l2Isolation03** in the **L2 Isolation** field, and select **macfilter03** in the **MAC Filtering** field. Click **Apply**.

3 Click the **Layer-2 Isolation** tab. When the **Layer-2 Isolation** screen appears, select **L2Isolation03**'s entry and click **Edit**. The following screen displays.

Figure 42 Tutorial: Layer-2 Isolation Edit



Enter the network switch's **MAC Address** and add a **Description** ("NET_SWITCH" in this case) in **Set 1**'s entry.

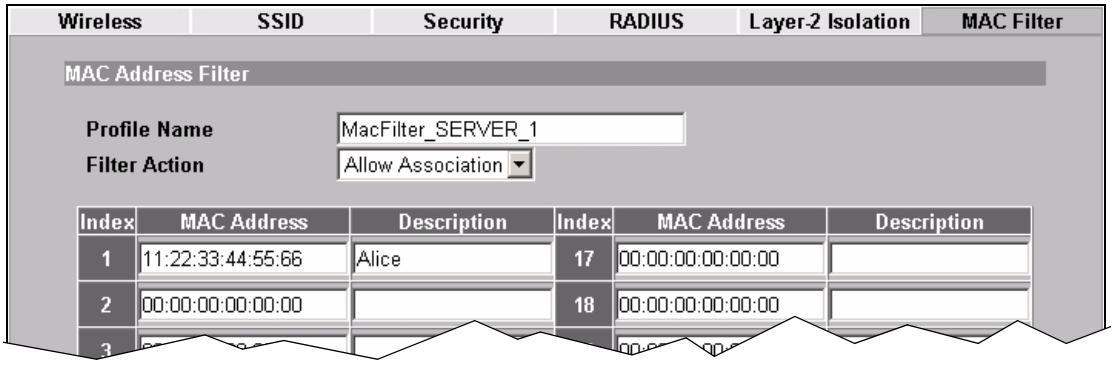
Enter server 1's **MAC Address** and add a **Description** ("SERVER_1" in this case) in **Set 2**'s entry.

Change the **Profile Name** to "L-2-ISO_SERVER_1" and click **Apply**. You have restricted users on the **SERVER_1** network to access only the devices with the MAC addresses you entered.

4 Click the **MAC Filter** tab. When the **MAC Filter** screen appears, select **macfilter03**'s entry and click **Edit**.

Enter the MAC address of the device Alice uses to connect to the network in **Index 1**'s **MAC Address** field and enter her name in the **Description** field, as shown in the following figure. Change the **Profile Name** to "MacFilter_SERVER_1". Select **Allow Association** from the **Filter Action** field and click **Apply**.

Figure 43 Tutorial: MAC Filter Edit (SERVER_1)



You have restricted access to the **SERVER_1** network to only the networking device whose MAC address you entered. The **SERVER_1** network is now configured.

5.4.5 Configure the SERVER_2 Network

Next, you will configure the **SERVER_2** network that allows Bob to access secure server **2** and the Internet.

To do this, repeat the procedure in Section 5.4.4 on page 77, substituting the following information.

Table 9 Tutorial: SERVER_2 Network Information

SSID Screen	
Index	4
Profile Name	SERVER_2
SSID Edit (SERVER_2) Screen	
L2 Isolation	L2Isolation04
MAC Filtering	macfilter04
Layer-2 Isolation (**L2Isolation04**) Screen	
Profile Name	L-2-ISO_SERVER-2
Set 1	MAC Address: 77:66:55:44:33:22 Description: NET_SWITCH
Set 2	MAC Address: 99:88:77:66:55:44 Description: SERVER_2
Set 3	MAC Address: 66:55:44:33:22:11 Description: GATEWAY
MAC Filter (**macfilter04**) Edit Screen	
Profile Name	MacFilter_SERVER_2
Set 1	MAC Address: 22:33:44:55:66:77 Description: Bob

5.4.6 Checking your Settings and Testing the Configuration

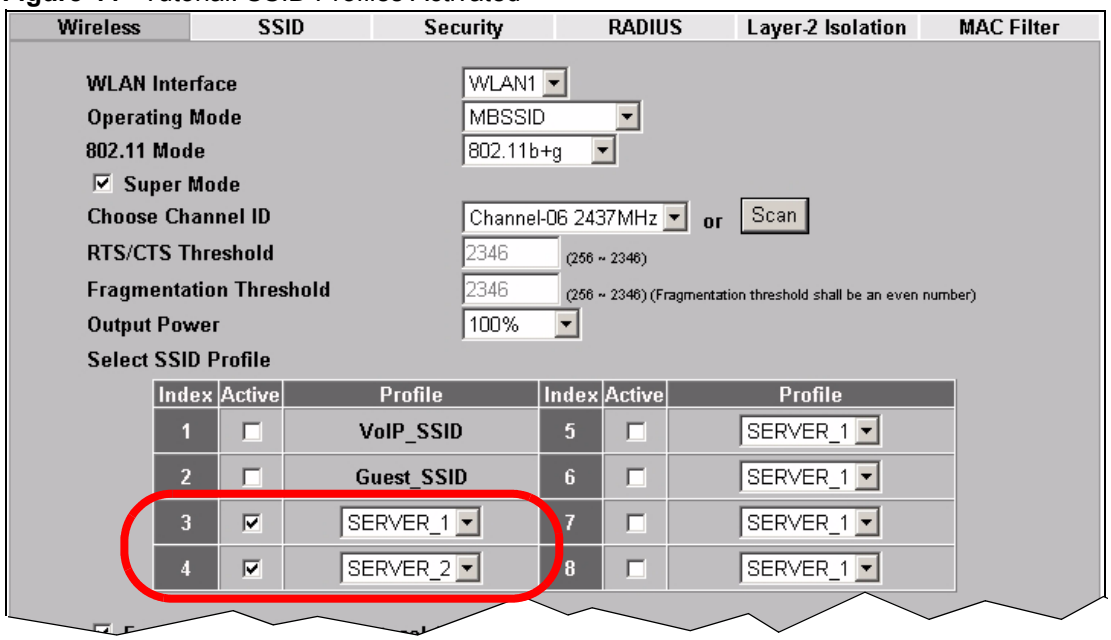
Use the following sections to ensure that your wireless networks are set up correctly.

5.4.6.1 Checking Settings

Take the following steps to check that the ZyXEL Device is using the correct SSIDs, MAC filters and layer-2 isolation profiles.

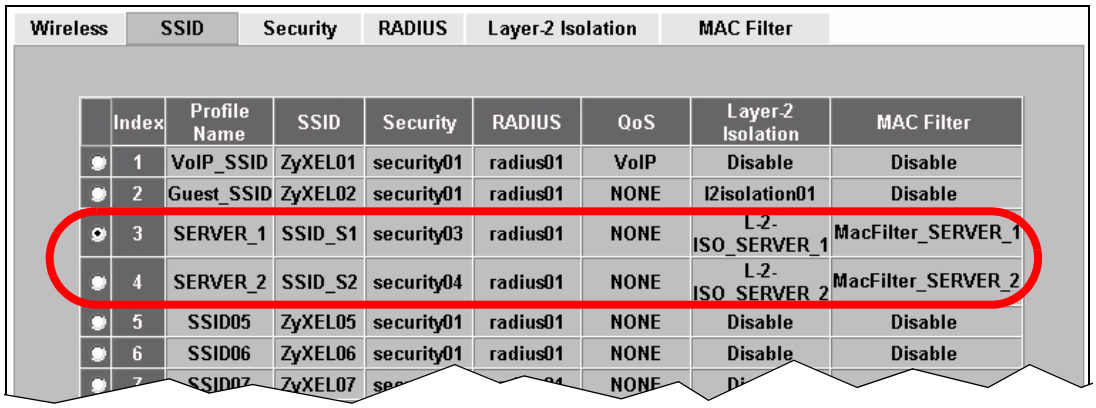
1 Click **WIRELESS > Wireless**. Check that the **Operating Mode** is **MBSSID** and that the correct SSID profiles are selected and activated, as shown in the following figure.

Figure 44 Tutorial: SSID Profiles Activated



2 Next, click the **SSID** tab. Check that each configured SSID profile uses the correct **Security**, **Layer-2 Isolation** and **MAC Filter** profiles, as shown in the following figure.

Figure 45 Tutorial: SSID Tab Correct Settings



If the settings are not as shown, follow the steps in the relevant section of this tutorial again.

5.4.6.2 Testing the Configuration

Before you allow employees to use the network, you need to thoroughly test whether the setup behaves as it should. Take the following steps to do this.

1 Test the **SERVER_1** network.

- Using Alice's computer and wireless client, and the correct security settings, do the following.

  Attempt to access Server **1**. You should be able to do so.

Attempt to access the Internet. You should be able to do so.
Attempt to access Server **2**. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.

- Using Alice's computer and wireless client, and incorrect security settings, attempt to associate with the **SERVER_1** network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and wireless client, but with the correct security settings, attempt to associate with the **SERVER_1** network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

2 Test the **SERVER_2** network.

- Using Bob's computer and wireless client, and the correct security settings, do the following.

  Attempt to access Server **2**. You should be able to do so.
  Attempt to access the Internet. You should be able to do so.
  Attempt to access Server **1**. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.
- Using Bob's computer and wireless client, and incorrect security settings, attempt to associate with the **SERVER_2** network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and wireless client, but with the correct security settings, attempt to associate with the **SERVER_2** network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

If you cannot do something that you should be able to do, check the settings as described in Section 5.4.6.1 on page 80, and in the individual Security, layer-2 isolation and MAC filter profiles for the relevant network. If this does not help, see the Troubleshooting chapter in this User's Guide.

PART II
The Web Configurator

System Screens (85)
Wireless Configuration (91)
Wireless Security Configuration (109)
MBSSID and SSID (121)
Other Wireless Configuration (129)
IP Screen (141)
Rogue AP (145)
Remote Management Screens (151)
Internal RADIUS Server (169)
Certificates (177)
Log Screens (195)
VLAN (203)
Maintenance (221)

6

System Screens

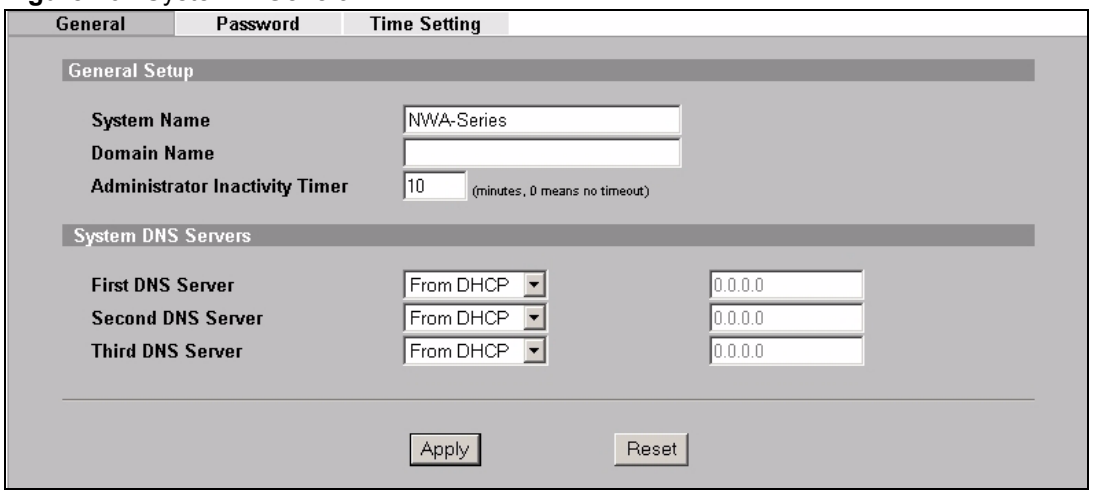
6.1 System Overview

This section provides information on general system setup.

6.2 Configuring General Setup

Click **SYSTEM** > **General**.

Figure 46 System > General



The following table describes the labels in this screen.

Table 10 System > General

LABEL	DESCRIPTION
General Setup	
System Name	Type a descriptive name to identify the ZyXEL Device in the Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).

Table 10 System > General

LABEL	DESCRIPTION
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From DHCP** if your DHCP server dynamically assigns DNS server information (and the ZyXEL Device's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is **None**.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.3 Administrator Authentication on RADIUS

The administrator authentication on RADIUS feature lets a (external or internal) RADIUS server authenticate management logins to the ZyXEL Device. This is useful if you need to regularly change a password that you use to manage several ZyXEL Devices.

Activate administrator authentication on RADIUS in the **SYSTEM > Password** screen and configure the same user name, password and RADIUS server information on each ZyXEL Device. Then, whenever you want to change the password, just change it on the RADIUS server.

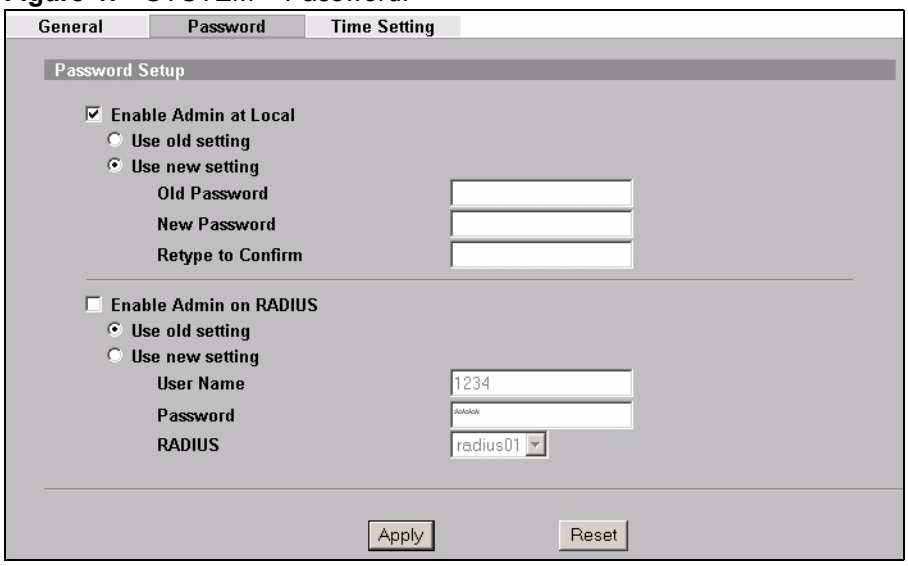
6.3.1 Configuring the Password

It is strongly recommended that you change your ZyXEL Device's password. Click **SYSTEM > Password**. The screen appears as shown.

If you forget your ZyXEL Device's password (or IP address), you will need to reset the device. See the section on resetting the ZyXEL Device for details

Regardless of how you configure this screen, you still use the local system password to log in via the console port (for internal use only).

Figure 47 SYSTEM > Password.



The following table describes the labels in this screen.

Table 11 Password

LABEL	DESCRIPTIONS
Enable Admin at Local	Select this check box to have the device authenticate management logins to the device.
Use old setting	Select this to have the ZyXEL Device use the local management password already configured on the device (“1234” is the default).
Use new setting	Select this if you want to change the local management password.
Old Password	Type in your existing system password (“1234” is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Enable Admin on RADIUS	Select this (and configure the other fields in this section) to have a RADIUS server authenticate management logins to the ZyXEL Device.
Use old setting	Select this to have a RADIUS server authenticate management logins to the ZyXEL Device using the RADIUS username and password already configured on the device.
Use new setting	Select this if you want to change the RADIUS username and password the ZyXEL Device uses to authenticate management logon.
User Name	Enter the username for this user account. This name can be up to 31 ASCII characters long, including spaces.
Password	Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. Spaces are allowed. Note: If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.

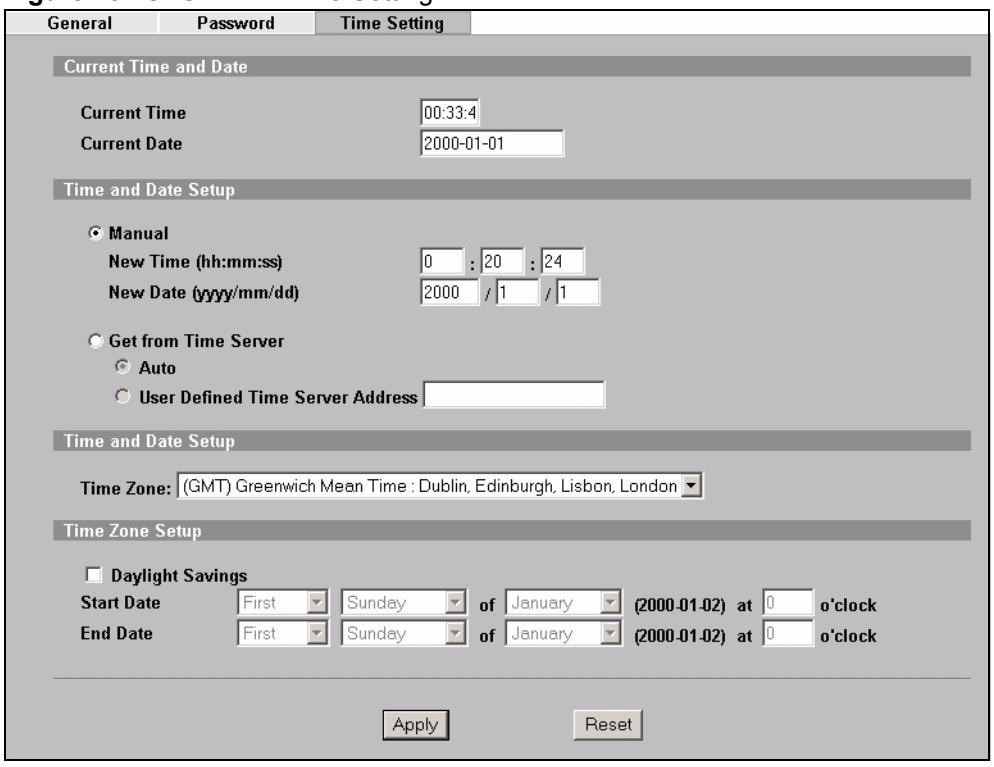
Table 11 Password

LABEL	DESCRIPTIONS
RADIUS	Select the RADIUS server profile of the RADIUS server that is to authenticate management logins to the ZyXEL Device. The ZyXEL Device tests the user name and password against the RADIUS server when you apply your settings. • The user name and password must already be configured in the RADIUS server. • You must already have a RADIUS profile configured for the RADIUS server (see Section 8.5 on page 119). • The server must be set to **Active** in the profile.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.4 Configuring Time Setting

To change your ZyXEL Device's time and date, click **SYSTEM** > **Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

Figure 48 SYSTEM > Time Setting



The following table describes the labels in this screen.

Table 12 SYSTEM > Time Setting

LABEL	DESCRIPTION
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server (if configured).
Current Date	This field displays the last updated date from the time server.
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy:mm:dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specify below.
Auto	Select this to have the ZyXEL Device use the predefined list of time servers.
User Defined Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/ network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Mar.**, **Last**, **Sun.** The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type "02" because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Oct.**, **Last**, **Sun**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 12 SYSTEM > Time Setting

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

6.5 Pre-defined NTP Time Servers List

When you turn on the ZyXEL Device for the first time, the date and time start at 2000-01-01 00:00:00. When you select **Auto** in the **SYSTEM** > **Time Setting** screen, the ZyXEL Device then attempts to synchronize with one of the following pre-defined list of NTP time servers.

The ZyXEL Device continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 13 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

When the ZyXEL Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyXEL Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

7

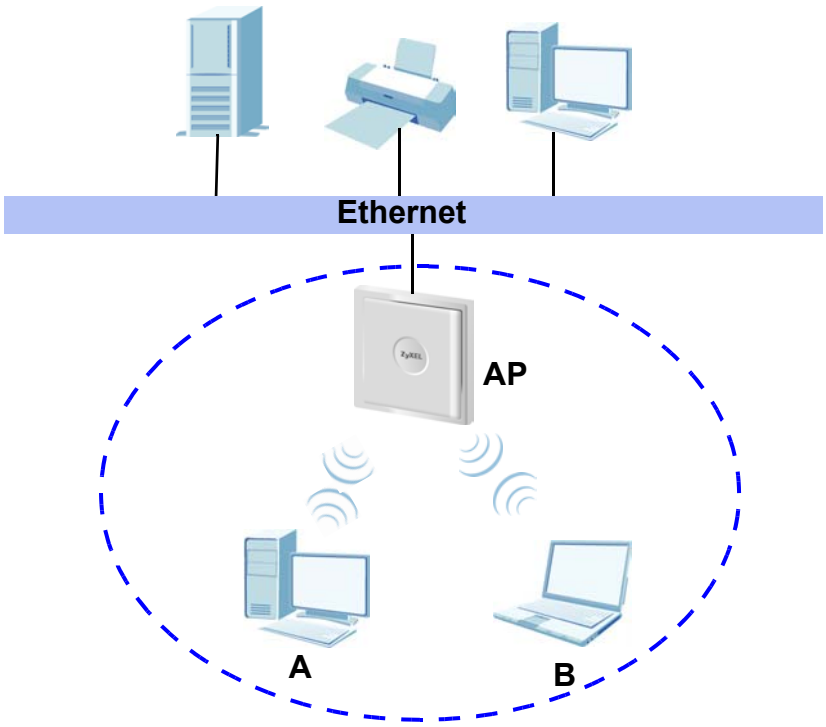
Wireless Configuration

This chapter discusses how to configure the ZyXEL Device's **Wireless** screens.

7.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 49 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

7.2 Wireless LAN Basics

See the Wireless LANs Appendix for information on the following:

- Wireless LAN Topologies
- Channel
- RTS/CTS
- Fragmentation Threshold
- IEEE 802.1x
- RADIUS
- Types of Authentication
- WPA
- Security Parameters Summary

7.3 Quality of Service

This section discusses the Quality of Service (QoS) features available on the ZyXEL Device.

7.3.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual and applications. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The ZyXEL Device uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q or DSCP information in each packet's header. The ZyXEL Device automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency and jitter (variations in delay).

7.3.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the ZyXEL Device uses.

Table 14 WMM QoS Priorities

PRIORITY LEVEL	DESCRIPTION
voice (WMM_VOICE)	Typically used for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality.
video (WMM_VIDEO)	Typically used for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.
best effort (WMM_BEST_EFFORT)	Typically used for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
background (WMM_BACKGROUND)	This is typically used for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements.

7.3.2 ATC

Automatic Traffic Classifier (ATC) is a bandwidth management tool that prioritizes data packets sent across the network. ATC assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency and a low level of jitter such as Voice over IP or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

ATC assigns priority based on packet size, since time-sensitive applications such as Internet telephony (Voice over IP or VoIP) tend to have smaller packet sizes than non-time sensitive applications such as FTP (File Transfer Protocol). The following table shows some common applications, their time sensitivity, and their typical data packet sizes. Note that the figures given are merely examples - sizes may differ according to application and circumstances.

Table 15 Typical Packet Sizes

APPLICATION	TIME SENSITIVITY	TYPICAL PACKET SIZE (BYTES)
Voice over IP (SIP)	High	< 250
Online Gaming	High	60 ~ 90
Web browsing (http)	Medium	300 ~ 600
FTP	Low	1500

When ATC is activated, the device sends traffic with smaller packets before traffic with larger packets if the network is congested.

ATC assigns priority to packets as shown in the following table.

Table 16 Automatic Traffic Classifier Priorities

PACKET SIZE (BYTES)	ATC PRIORITY
1 ~ 250	ATC_High
250 ~ 1100	ATC_Medium
1100 +	ATC_Low

You should activate ATC on the ZyXEL Device if your wireless network includes networking devices that do not support WMM QoS, or if you want to prioritize traffic but do not want to configure WMM QoS settings.

7.3.3 ATC+WMM

The ZyXEL Device can use a mapping mechanism to use both ATC and WMM QoS. The ATC+WMM function prioritizes all packets transmitted onto the wireless network using WMM QoS, and prioritizes all packets transmitted onto the wired network using ATC. See Section 9.2.2 on page 127 for details of how to configure ATC+WMM.

Use the ATC+WMM function if you want to do the following:

- enable WMM QoS on your wireless network and automatically assign a WMM priority to packets that do not already have one (see Section 7.3.3.1 on page 94).
- automatically prioritize all packets going from your wireless network to the wired network (see Section 7.3.3.2 on page 94).

7.3.3.1 ATC+WMM from LAN to WLAN

ATC+WMM from LAN (the wired Local Area Network) to WLAN (the Wireless Local Area Network) allows WMM prioritization of packets that do not already have WMM QoS priorities assigned. The ZyXEL Device automatically classifies data packets using ATC and then assigns WMM priorities based on that ATC classification.

The following table shows how priorities are assigned for packets coming from the LAN to the WLAN.

Table 17 ATC + WMM Priority Assignment (LAN to WLAN)

PACKET SIZE (BYTES)	→	ATC VALUE	→	WMM VALUE
1 ~ 250		ATC_High		WMM_VIDEO
250 ~ 1100		ATC_Medium		WMM_BEST_EFFORT
1100 +		ATC_Low		WMM_BACKGROUND

7.3.3.2 ATC+WMM from WLAN to LAN

ATC+WMM from WLAN to LAN automatically prioritizes (assigns an ATC value to) all packets coming from the WLAN. Packets are assigned an ATC value based on their WMM value, not their size.

The following table shows how priorities are assigned for packets coming from the WLAN to the LAN when using ATC+WMM.

Table 18 ATC + WMM Priority Assignment (WLAN to LAN)

WMM VALUE	→	ATC VALUE
WMM_VOICE		ATC_High
WMM_VIDEO		ATC_High
WMM_BEST_EFFORT		ATC_Medium
WMM_BACKGROUND		ATC_Low
NONE		ATC_Medium

7.3.4 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

7.3.4.1 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

7.3.4.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

Figure 50 DiffServ: Differentiated Service Field

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

7.3.5 ToS (Type of Service) and WMM QoS

The DSCP value of outgoing packets is between 0 and 255. 0 is the default priority. WMM QoS checks the DSCP value in the header of data packets. It gives the traffic a priority according to this number.

In order to control which priority level is given to traffic, the device sending the traffic must set the DSCP value in the header. If the DSCP value is not specified, then the traffic is treated as best-effort. This means the wireless clients and the devices with which they are communicating must both set the DSCP value in order to make the best use of WMM QoS. A Voice over IP (VoIP) device for example may allow you to define the DSCP value.

The following table lists which WMM QoS priority level the ZyXEL Device uses for specific DSCP values.

Table 19 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping

DSCP VALUE	WMM QOS PRIORITY LEVEL
224, 192	voice
160, 128	video
96, 0 [A]	besteffort
64, 32	background

A. The ZyXEL Device also uses best effort for any DSCP value for which another WMM QoS priority is not specified (255, 158 or 37 for example).

7.4 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

7.4.1 Rapid STP

The ZyXEL Device uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

7.4.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the following table.

Table 20 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

7.4.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

7.4.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 21 STP Port States

PORT STATES	DESCRIPTIONS
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

7.5 DFS

When you choose **802.11a** in **Access Point**, **Bridge/Repeater** or **AP + Bridge** mode, the ZyXEL Device uses DFS (Dynamic Frequency Selection) to give you a wider choice of wireless channels.

DFS allows you to use channels in the frequency range normally reserved for radar systems. Radar uses radio signals to detect the location of objects for military, meteorological or air traffic control purposes. As long as your ZyXEL Device detects no radar activity on the channel you select, you can use the channel to communicate. However, a wireless LAN operating on the same frequency as an active radar system could disrupt the radar system. Therefore, if the ZyXEL Device detects radar activity on the channel you select, it automatically instructs the wireless clients to move to another channel, then resumes communications on the new channel.

7.6 Wireless Screen Overview

The following is a list of the wireless screens you can configure on the ZyXEL Device.

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter

1. Configure the ZyXEL Device to operate in AP, Bridge/Repeater, AP+Bridge or MBSSID mode in the **Wireless** screen. You can also select an **SSID Profile** in the **Wireless** screen.
2. Use the **SSID** screens to view and edit SSID profiles.
3. Use the **Security** screen to configure wireless security profiles.
4. Use the **RADIUS** screen to configure RADIUS authentication and accounting settings.
5. Use the **Layer-2 Isolation** screen to prevent wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.
6. Use the **MAC Filter** screen to allow or restrict access to your wireless network based on a client's MAC address.

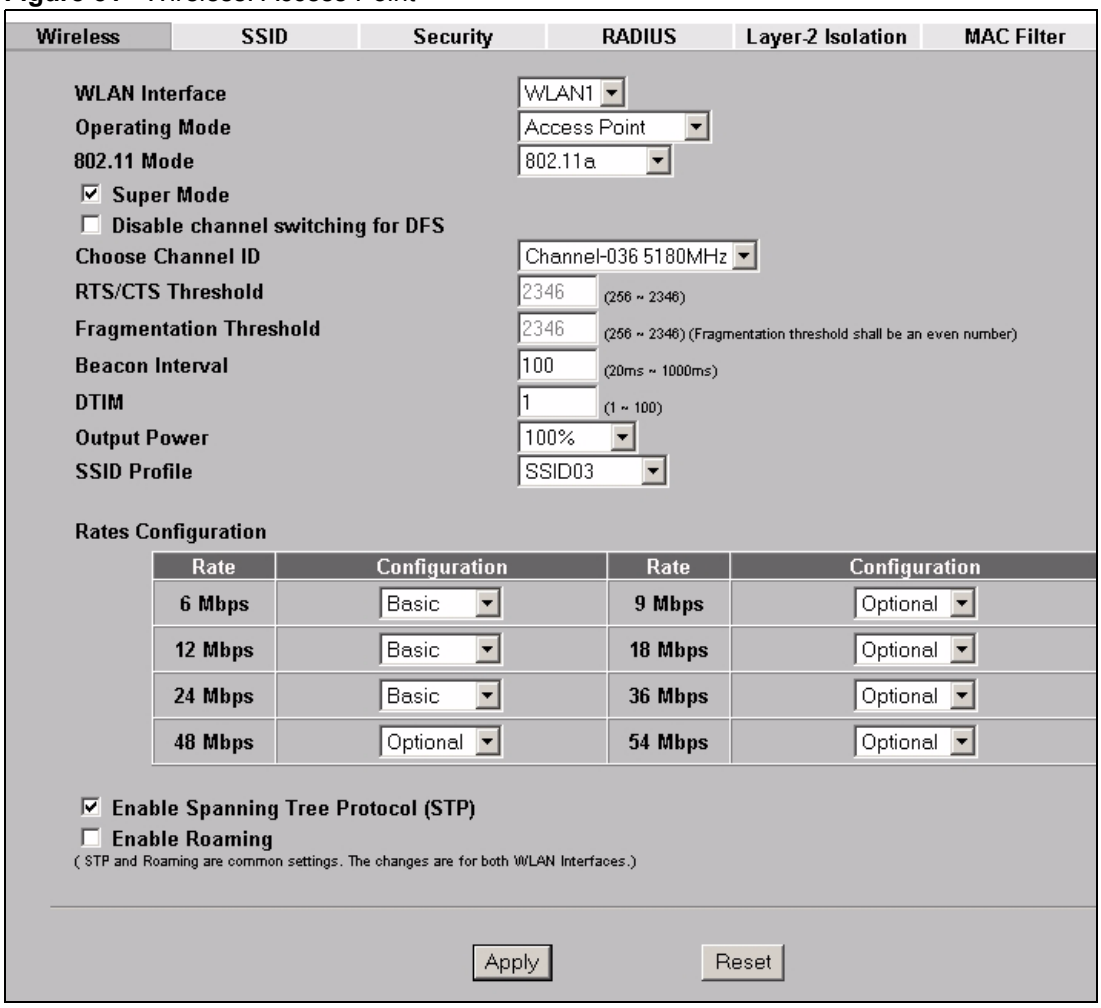
7.7 Configuring Wireless Settings

Click **WIRELESS > Wireless**. The screen varies depending upon the operating mode you select.

7.7.1 Access Point Mode

Select **Access Point** as the **Operating Mode** to display the screen shown next.

Figure 51 Wireless: Access Point



The following table describes the general wireless LAN labels in this screen.

Table 22 Wireless: Access Point

LABEL	DESCRIPTION
WLAN Interface	Select which WLAN adapter you want to configure. It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.
Operating Mode	Select **Access Point** from the drop-down list.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11a** to allow only IEEE 802.11a compliant WLAN devices to associate with the ZyXEL Device.
Super Mode	Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting.

Table 22 Wireless: Access Point

LABEL	DESCRIPTION
Disable channel switching for DFS	This field displays only when you select **802.11a** in the **802.11 Mde** field. Select this if you do not want to use DFS (Dynamic Frequency Selection).
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyXEL Device automatically select a channel, click **Scan** instead.
Scan	Click this button to have the ZyXEL Device automatically scan for and select the channel with the least interference.
Disable channel switching for DFS	This field is available when you select **802.11a** in the **802.11 Mode** field. DFS (dynamic frequency selection) allows an AP to detect other devices in the same channel. If there is another device using the same channel, the AP changes to a different channel, so that it can avoid interference with radar systems or other wireless networks. Select this option to disable DFS on the ZyXEL Device when **802.11 Mode** is set to **802.11a**.
RTS/CTS Threshold	The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its smallest value (256) turns on the RTS/CTS handshake. Enter a value between **256** and **2346**. This field is not available when **Super Mode** is selected.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**. This field is not available when **Super Mode** is selected.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select one of the following **100%**, **50%**, **25%**, **12.5%** or **Minimum**. See the product specifications for more information on your ZyXEL Device's output power. This field is not available when you select **802.11a** in the **802.11 Mode** field.

Table 22 Wireless: Access Point

LABEL	DESCRIPTION
SSID Profile	The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Select an **SSID Profile** from the drop-down list box. Configure SSID profiles in the **SSID** screen (see Section 9.2 on page 125 for information on configuring SSID). Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Rates Configuration	This section controls the data rates permitted for clients. For each **Rate**, select an option from the **Configuration** list. The options are: • **Basic** (1~11 Mbps only): Clients can always connect to the access point at this speed. • **Optional**: Clients can connect to the access point at this speed, when permitted to do so by the AP. • **Disabled**: Clients cannot connect to the access point at this speed.
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select this to activate STP on the ZyXEL Device.
Enable Roaming	Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this to enable roaming on the ZyXEL Device if you have two or more ZyXEL Devices on the same subnet. Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

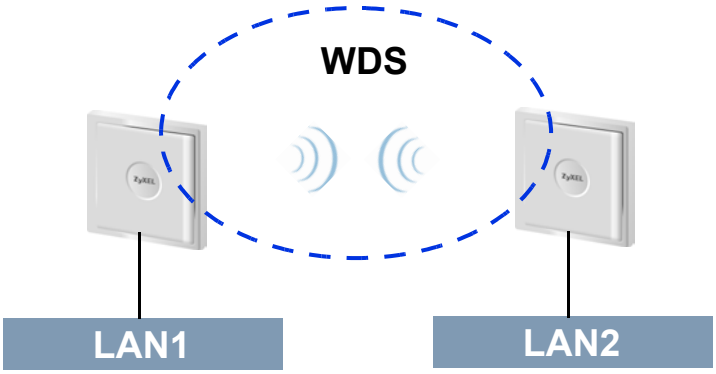
7.7.2 Bridge/Repeater Mode

The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

The ZyXEL Device can establish up to five wireless links with other APs.

In the example below, when both ZyXEL Devices are in **Bridge/Repeater** mode, they form a WDS (Wireless Distribution System) allowing the computers in **LAN 1** to connect to the computers in **LAN 2**.

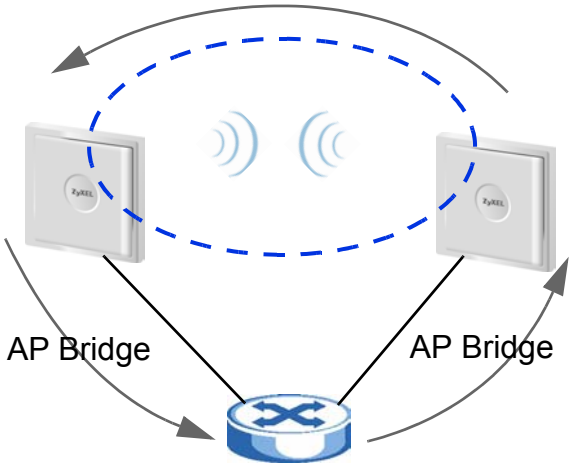
Figure 52 Bridging Example



Be careful to avoid bridge loops when you enable bridging in the ZyXEL Device. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

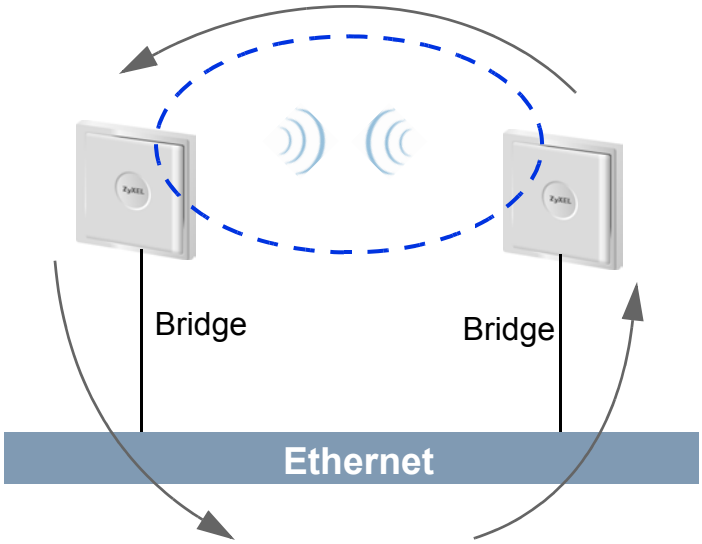
- If two or more ZyXEL Devices (in bridge mode) are connected to the same hub.

Figure 53 Bridge Loop: Two Bridges Connected to Hub



- If your ZyXEL Device (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN.

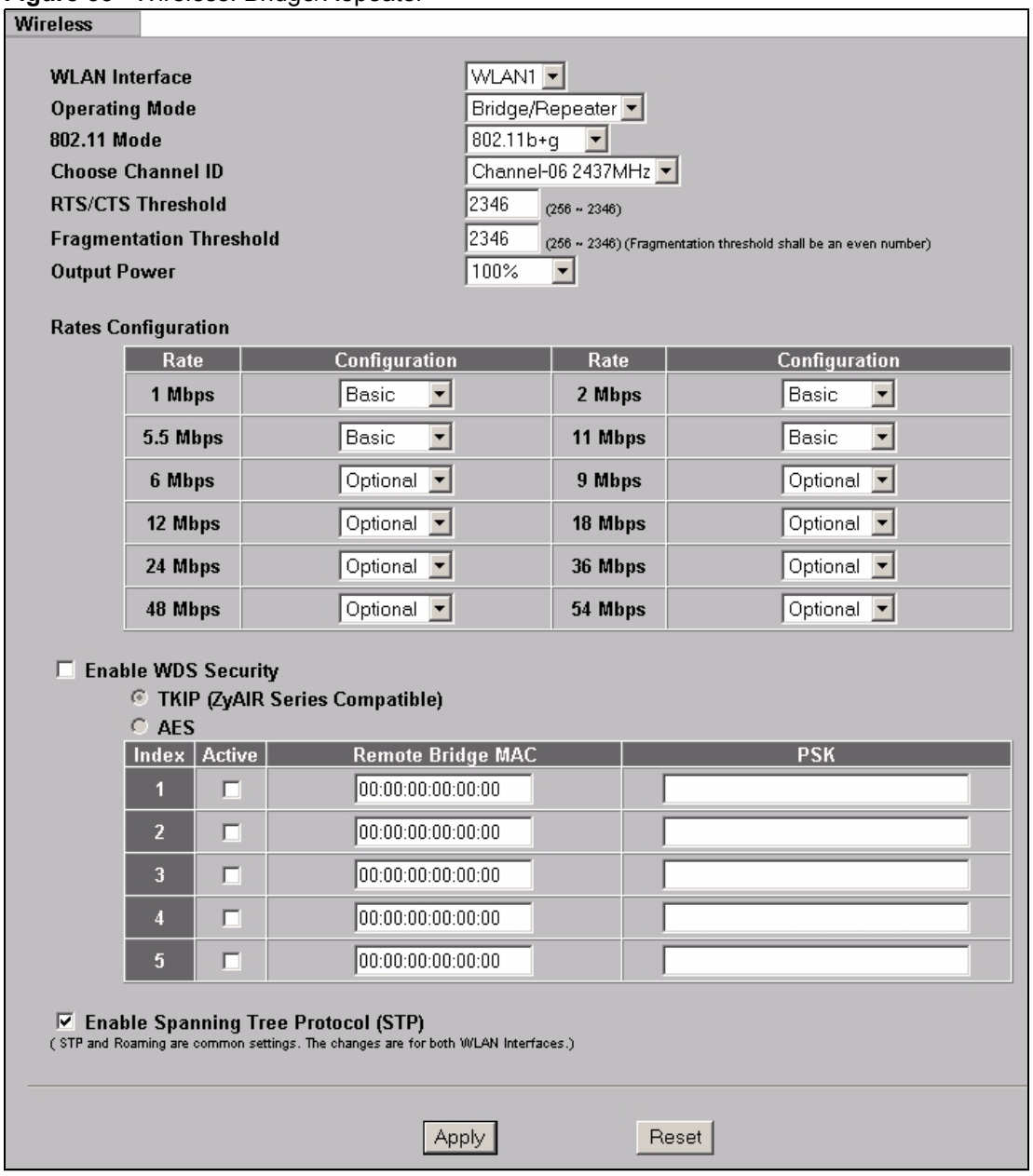
Figure 54 Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that you enable STP in the **Wireless** screen or your ZyXEL Device is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

To have the ZyXEL Device act as a wireless bridge only, click **WIRELESS** > **Wireless** and select **Bridge/Repeater** as the **Operating Mode**.

Figure 55 Wireless: Bridge/Repeater



The following table describes the bridge labels in this screen.

Table 23 Wireless: Bridge/Repeater

LABEL	DESCRIPTIONS
WLAN Interface	Select which WLAN adapter you want to configure. It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.
Operating Mode	Select **Bridge/Repeater** in this field.

Table 23 Wireless: Bridge/Repeater

LABEL	DESCRIPTIONS
802.11 mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11a** to allow only IEEE 802.11a compliant WLAN devices to associate with the ZyXEL Device.
Disable channel switching for DFS	This field displays only when you select **802.11a** in the **802.11 Mde** field. Select this if you do not want to use DFS (Dynamic Frequency Selection).
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.
RTS/CTS Threshold	The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **256** and **2346**.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select from **100%**, **50%**, **25%**, **12.5%** and **Minimum**. See the product specifications for more information on your ZyXEL Device's output power. This field is not available when you select **802.11a** in the **802.11 Mode** field.
Enable WDS Security	Select this to turn on security for the ZyXEL Device's Wireless Distribution System (WDS). A Wireless Distribution System is a wireless connection between two or more APs. If you do not select the check box, traffic between APs is not encrypted. Note: WDS security is independent of the security settings between the ZyXEL Device and any wireless clients. When you enable WDS security, also do the following: • Select the type of security you want to use (**TKIP** or **AES**) to secure traffic on your WDS. • Enter a pre-shared key in the **PSK** field for each access point in your WDS. Each access point can use a different pre-shared key. • Configure WDS security and the relevant PSK in each of your other access point(s). Note: Other APs must use the same encryption method to enable WDS security.

Table 23 Wireless: Bridge/Repeater

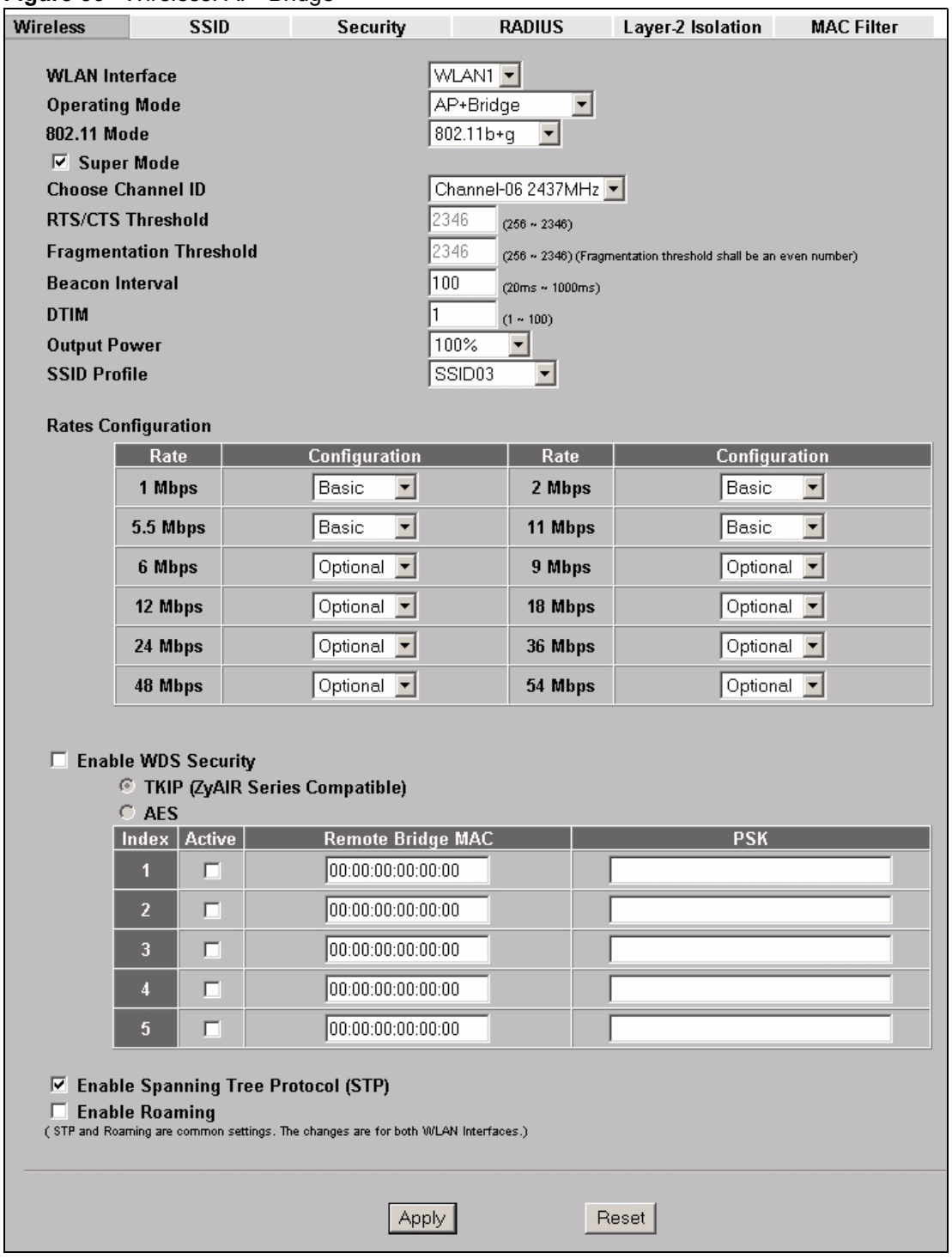
LABEL	DESCRIPTIONS
TKIP (ZyAIR Series Compatible)	Select this to enable Temporal Key Integrity Protocol (TKIP) security on your WDS. This option is compatible with other ZyXEL access points including that support WDS security. Use this if the other access points on your network support WDS security but do not have an AES option. Note: Check your other AP's documentation to make sure it supports WDS security. Note: At the time of writing, this option is compatible with other ZyXEL NWA Series and G-3000/G-3000H access points only.
AES	Select this to enable Advanced Encryption System (AES) security on your WDS. AES provides superior security to TKIP. Use AES if the other access points on your network support it for the WDS. Note: At the time of writing, this option is compatible with other ZyXEL NWA Series access points only.
Index	This is the index number of the bridge connection.
Active	Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.
Remote Bridge MAC Address	Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
PSK	Type a pre-shared key (PSK) from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). You must also set the peer device to use the same pre-shared key. Each peer device can use a different pre-shared key.

See Table 22 on page 99 for information on the other labels in this screen.

7.7.3 AP+Bridge Mode

Select **AP+Bridge** as the **Operating Mode** in the **WIRELESS** > **Wireless** screen to have the ZyXEL Device function as a bridge and access point simultaneously. See the section on applications for more information.

Figure 56 Wireless: AP+Bridge



See the tables describing the fields in the **Access Point** and **Bridge/Repeater** operating modes for descriptions of the fields in this screen.

7.7.4 MBSSID Mode

Select **MBSSID** as the **Operating Mode**. Refer to Chapter 9 on page 121 for configuration instructions and detailed information. See Chapter 8 on page 109 for details on the security settings.

8

Wireless Security Configuration

This chapter describes how to use the **Security** and **RADIUS** screens to configure wireless security on your ZyXEL Device.

8.1 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

8.1.1 SSID

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

8.1.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

8.1.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

8.1.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 8.1.3 on page 110 for information about this.)

Table 24 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	
↕	Static WEP	
	WPA-PSK	WPA
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no security, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **WEP** in the wireless network.

It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you use WPA2 or WPA2-PSK in your ZyXEL Device, you can select **WPA2-MIX** or **WPA2-PSK-MIX** to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK-MIX** or **WPA2-MIX** (depending on the type of wireless network login) in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the same wireless network must have the same key.

8.2 Security Modes

The following table describes the security modes you can configure.

Table 25 Security Modes

SECURITY MODE	DESCRIPTION
None	Select this to have no data encryption.
WEP	Select this to use WEP encryption.
802.1x-Only	Select this to use 802.1x authentication with no data encryption.
802.1x-Static64	Select this to use 802.1x authentication with a static 64bit WEP key and an authentication server.
802.1x-Static128	Select this to use 802.1x authentication with a static 128bit WEP key and an authentication server.
WPA	Select this to use WPA.
WPA-PSK	Select this to use WPA with a pre-shared key.
WPA2	Select this to use WPA2.
WPA2-MIX	Select this to use either WPA2 or WPA depending on which security mode the wireless client uses.
WPA2-PSK	Select this to use WPA2 with a pre-shared key.
WPA2-PSK-MIX	Select this to use either WPA-PSK or WPA2-PSK, depending on which security mode the wireless client uses.

8.3 Configuring Security

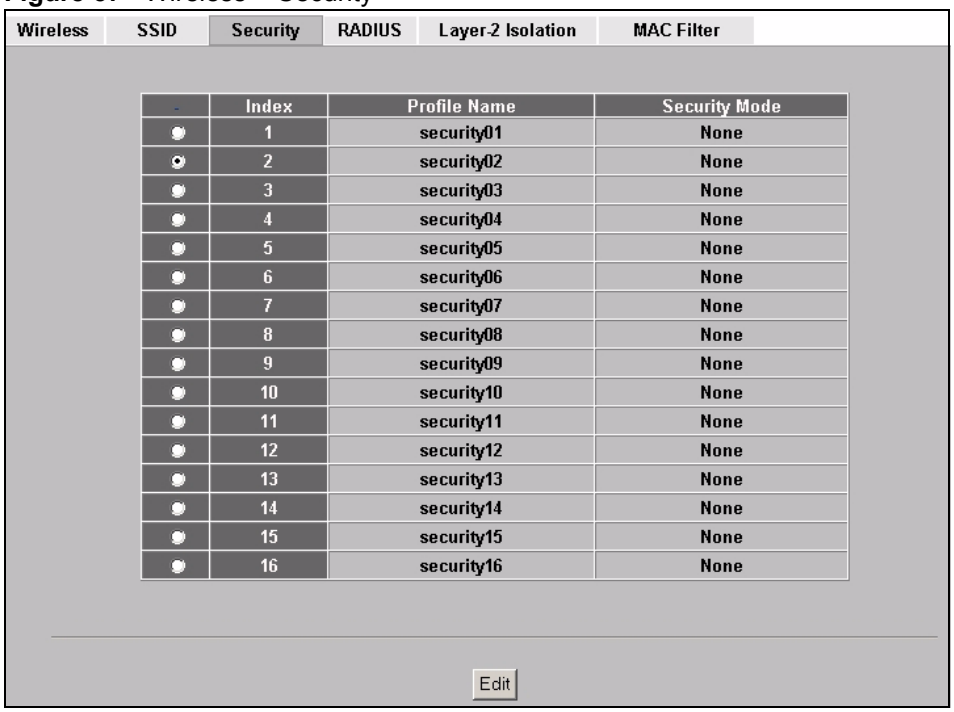
The following screens are configurable only in **Access Point**, **AP+Bridge** and **MBSSID** operating modes only.

Use the **Security** screen to create secure profiles. A security profile is a group of configuration settings which can be assigned to an SSID profile in the **SSID** configuration screen.

You can configure up to 16 security profiles.

To change your ZyXEL Device's wireless security settings, click **WIRELESS** > **Security**.

Figure 57 Wireless > Security



The following table describes the labels in this screen.

Table 26 WIRELESS > Security

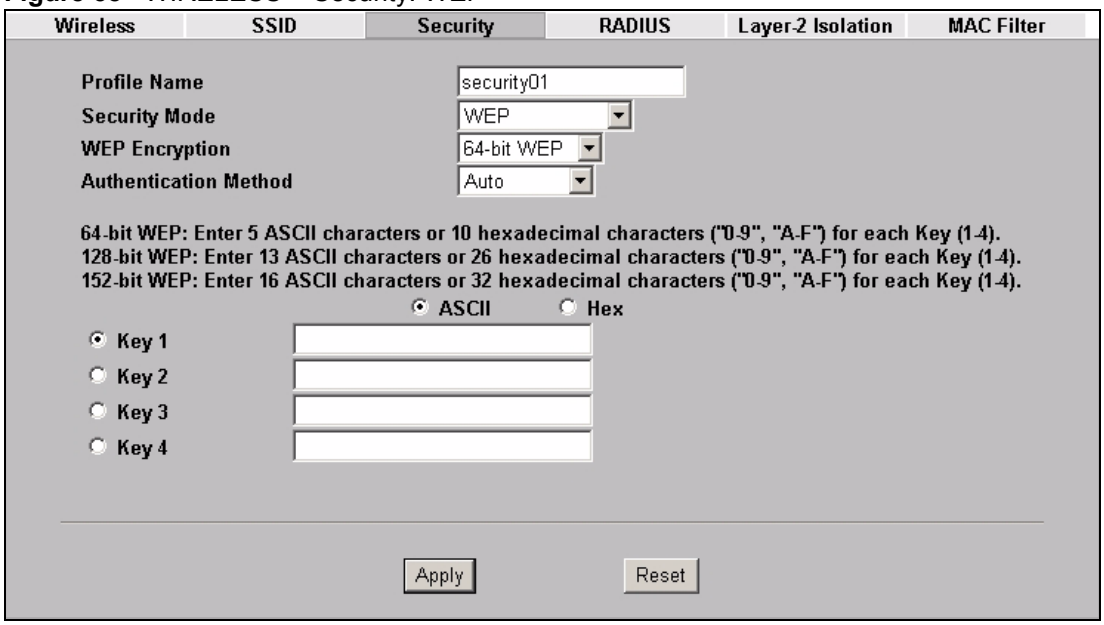
LABEL	DESCRIPTION
Index	This is the index number of the security profile.
Profile Name	This field displays a name given to a security profile in the **Security** configuration screen.
Security Mode	This field displays the security mode this security profile uses.
Edit	Select an entry from the list and click **Edit** to configure security settings for that profile.

The next screen varies according to the **Security Mode** you select.

8.3.1 Security: WEP

Select **WEP** in the **Security Mode** field to display the following screen.

Figure 58 WIRELESS > Security: WEP



The following table describes the labels in this screen.

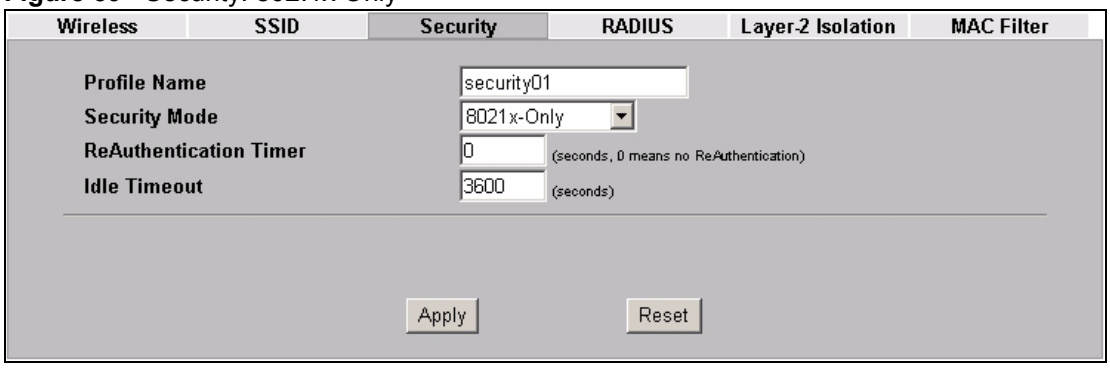
Table 27 Security: WEP

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose **WEP** in this field.
WEP Encryption	Select **64-bit WEP**, **128-bit WEP** or **152-bit WEP** to enable data encryption.
Authentication Method	Select **Auto** or **Shared Key** from the drop-down list box. The default setting is **Auto**.
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding “0x” is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **152-bit WEP**, then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.3.2 Security: 802.1x Only

Select **8021x-Only** in the **Security Mode** field to display the following screen.

Figure 59 Security: 802.1x Only



The following table describes the labels in this screen.

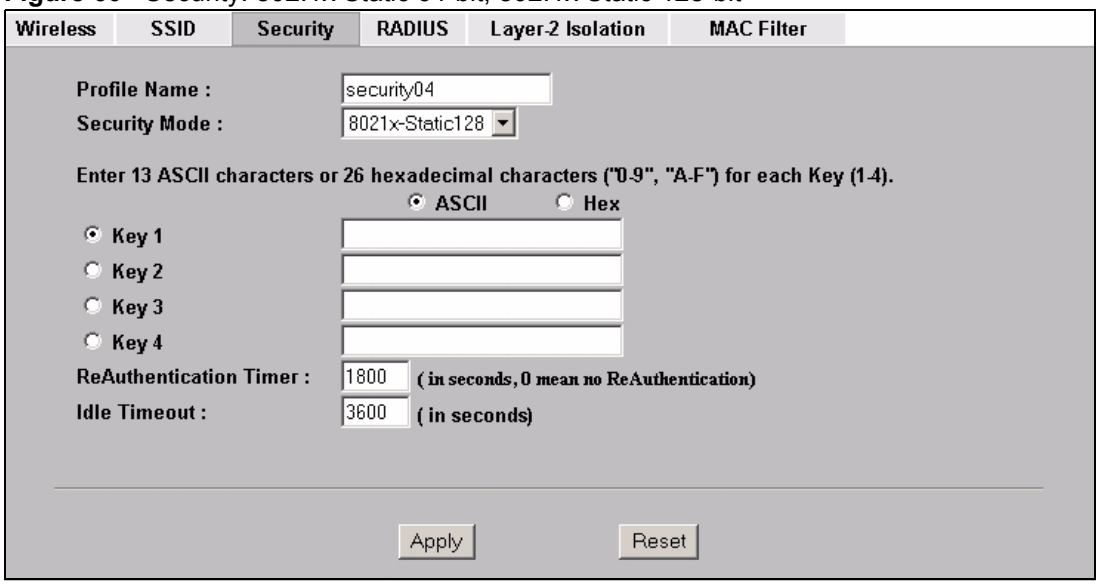
Table 28 Security: 802.1x Only

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose **8021x-Only** in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter “0” to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.3.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

Select **8021x-Static64** or **8021x-Static128** in the **Security Mode** field to display the following screen.

Figure 60 Security: 802.1x Static 64-bit, 802.1x Static 128-bit



The following table describes the labels in this screen.

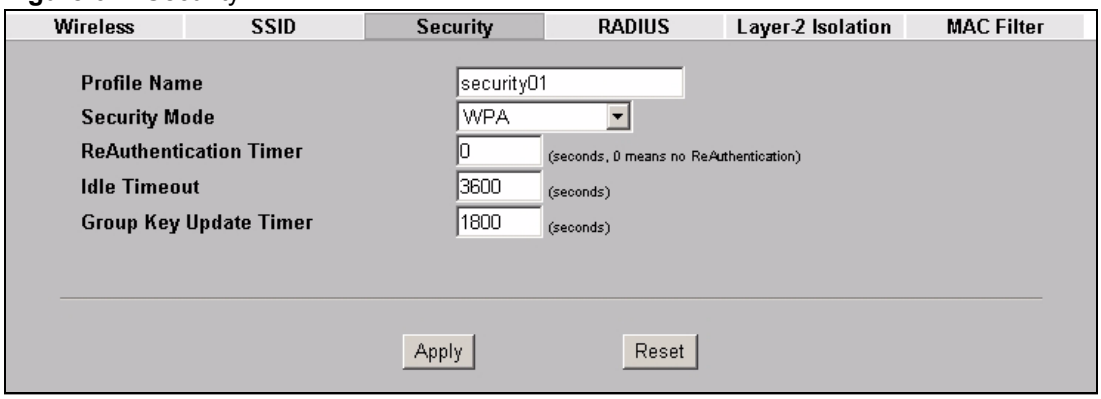
Table 29 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose **8021x-Static64 or 8021x-Static128** in this field.
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys.The preceding “0x” is entered automatically.
Key 1 to Key 4	If you chose **802.1x Static 64**, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **802.1x Static 128-bit**, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations. The preceding “0x” is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter “0” to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.3.4 Security: WPA

Select **WPA** in the **Security Mode** field to display the following screen.

Figure 61 Security: WPA



The following table describes the labels in this screen.

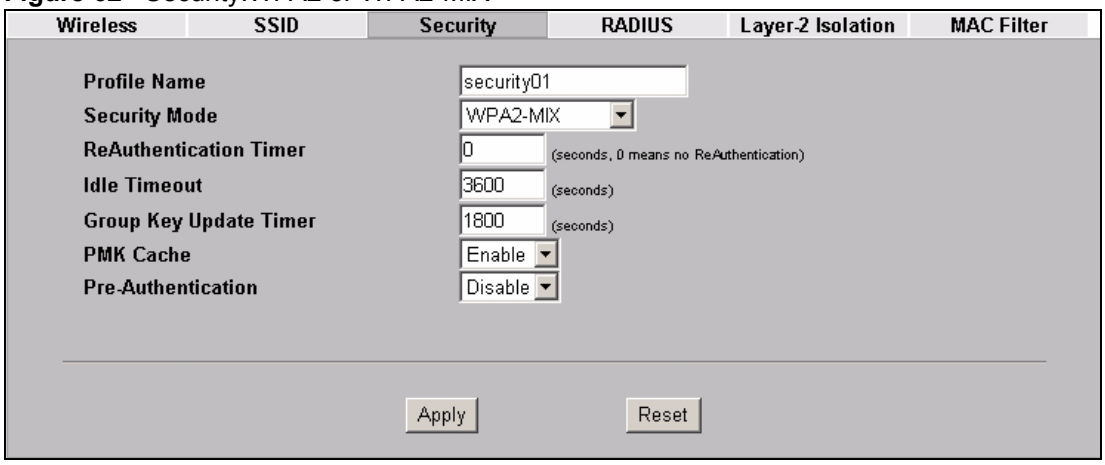
Table 30 Security: WPA

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Choose **WPA** in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter “0” to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.3.5 Security: WPA2 or WPA2-MIX

Select **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 62 Security:WPA2 or WPA2-MIX



The following table describes the labels not previously discussed

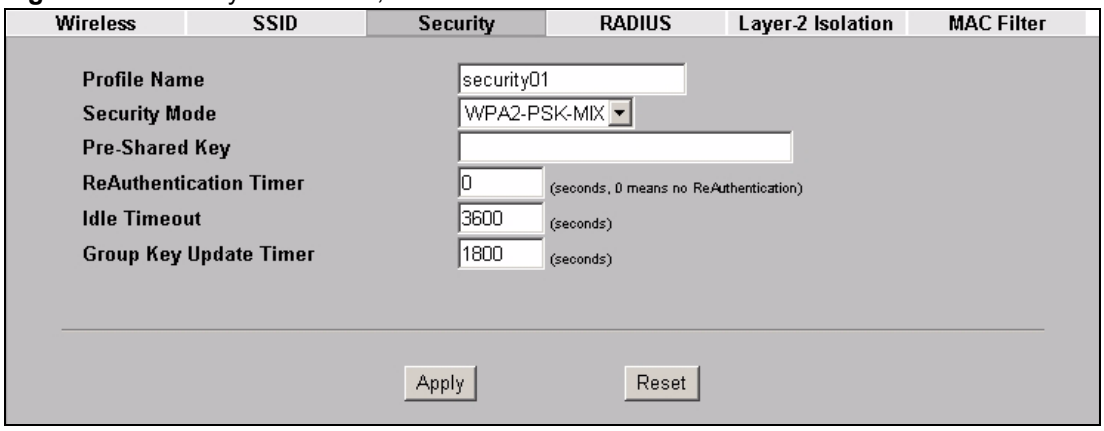
Table 31 Security: WPA2 or WPA2-MIX

LABEL	DESCRIPTIONS
Profile Name	Type a name to identify this security profile.
Security Mode	Choose **WPA2** or **WPA2-MIX** in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter “0” to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device‘s default is 1800 seconds (30 minutes).
PMK Cache	When a wireless client moves from one AP’s coverage area to another, it performs an authentication procedure (exchanging security information) with the new AP. Instead of re-authenticating a client each time it returns to the AP’s coverage area, which can cause delays to time-sensitive applications, the AP and the client can store (or “cache”) and use information about their previous authentication. Select **Enable** to allow PMK caching, or **Disable** to switch this feature off.
Pre-Authentication	Pre-authentication allows a wireless client to perform authentication with a different AP from the one to which it is currently connected, before moving into the new AP’s coverage area. This speeds up roaming. Select **Enable** to allow pre-authentication, or **Disable** to switch it off.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.3.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in the **Security Mode** field to display the following screen.

Figure 63 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX



The following table describes the labels not previously discussed

Table 32 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter “0” to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device’s default is 1800 seconds (30 minutes).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4 Introduction to RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where the access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks, among others:

- Authentication
  Determines the identity of the users.
- Accounting
  Keeps track of the client's network activity.

The ZyXEL Device is equipped with an internal RADIUS server. See Section 14.1 on page 169 for more details.

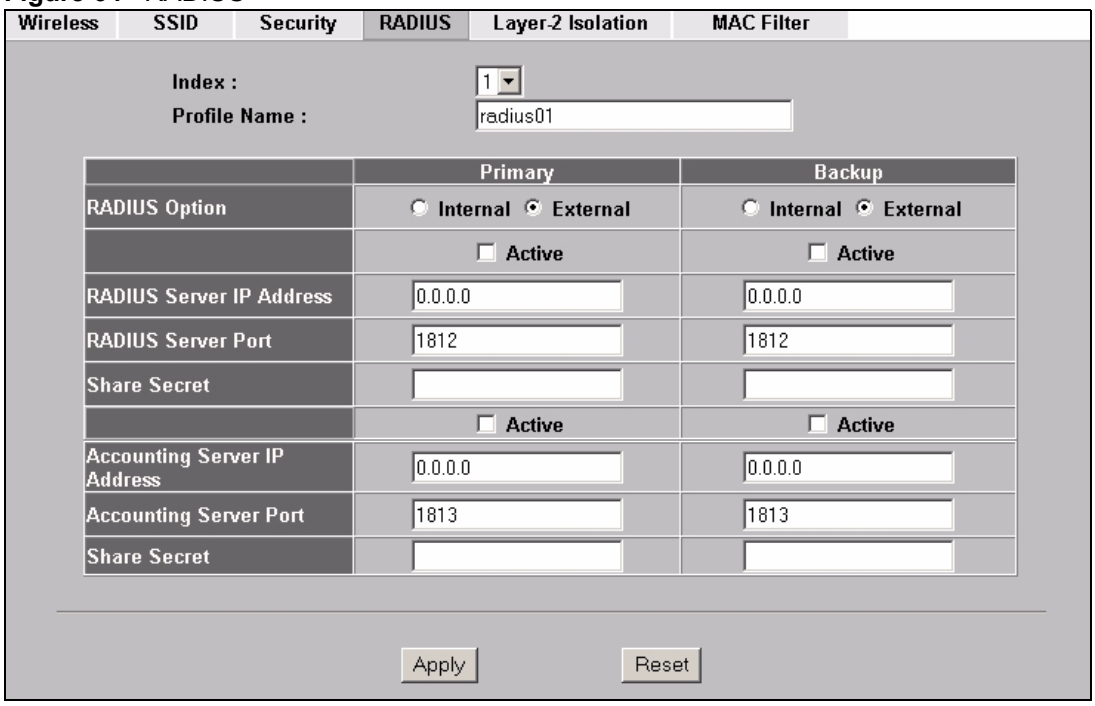
8.5 Configuring RADIUS

Use RADIUS if you want to authenticate wireless users using the internal authentication server (see Section 14.1 on page 169) or an external server.

You can configure up to four RADIUS server profiles. Each profile also has one backup authentication server and a backup accounting server. These profiles can be assigned to an SSID profile in the **SSID** configuration screen

To set up your ZyXEL Device's RADIUS server settings, click **WIRELESS** > **RADIUS**. The screen appears as shown.

Figure 64 RADIUS



The following table describes the labels in this screen.

Table 33 RADIUS

LABEL	DESCRIPTION
Index	Select the RADIUS profile you want to configure from the drop-down list box.
Profile Name	Type a name for the RADIUS profile associated with the **Index** number above.
Primary	Configure the fields below to set up user authentication and accounting.
Backup	If the ZyXEL Device cannot communicate with the **Primary** accounting server, you can have the ZyXEL Device use a **Backup** RADIUS server. Make sure the **Active** check boxes are selected if you want to use backup servers. The ZyXEL Device will attempt to communicate three times before using the **Backup** servers. Requests can be issued from the client interface to use the backup server. The length of time for each authentication is decided by the wireless client or based on the configuration of the **ReAuthentication Timer** field in the **Security** screen.
RADIUS Option	
Internal	Select this check box to use the ZyXEL Device's internal authentication server. The **Active**, **RADIUS Server IP Address**, **RADIUS Server Port** and **Share Secret** fields are not available when you use the internal authentication server.
External	Select this check box to use an external authentication server. The ZyXEL Device does not use the internal authentication server when this check box is enabled.
Active	Select the check box to enable user authentication through an external authentication server. This check box is not available when you select **Internal**.
RADIUS Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation. This field is not available when you select **Internal**.
RADIUS Server Port	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so. This field is not available when you select **Internal**.
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network. This field is not available when you select **Internal**.
Active	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

9

MBSSID and SSID

This chapter describes how to configure and use your ZyXEL Device's MBSSID mode and configure SSID profiles.

9.1 Wireless LAN Infrastructures

See the Wireless LAN chapter for some basic WLAN scenarios and terminology.

9.1.1 MBSSID

Traditionally, you needed to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there was also the possibility of channel interference. The ZyXEL Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying levels of privilege to different SSIDs.

Wireless stations can use different BSSIDs to associate with the same AP.

9.1.2 Notes on Multiple BSS

- There is a maximum number of BSSs allowed on one AP simultaneously.
  On the NWA-3160 and NWA-3163, a maximum of eight simultaneous BSSs are allowed.
  On the NWA-3165, a maximum of four simultantious BSSs are allowed.
- You must use different WEP keys for different BSSs. If two stations have different BSSIDs (they are in different BSSs), but have the same WEP keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

9.1.3 Multiple BSS Example

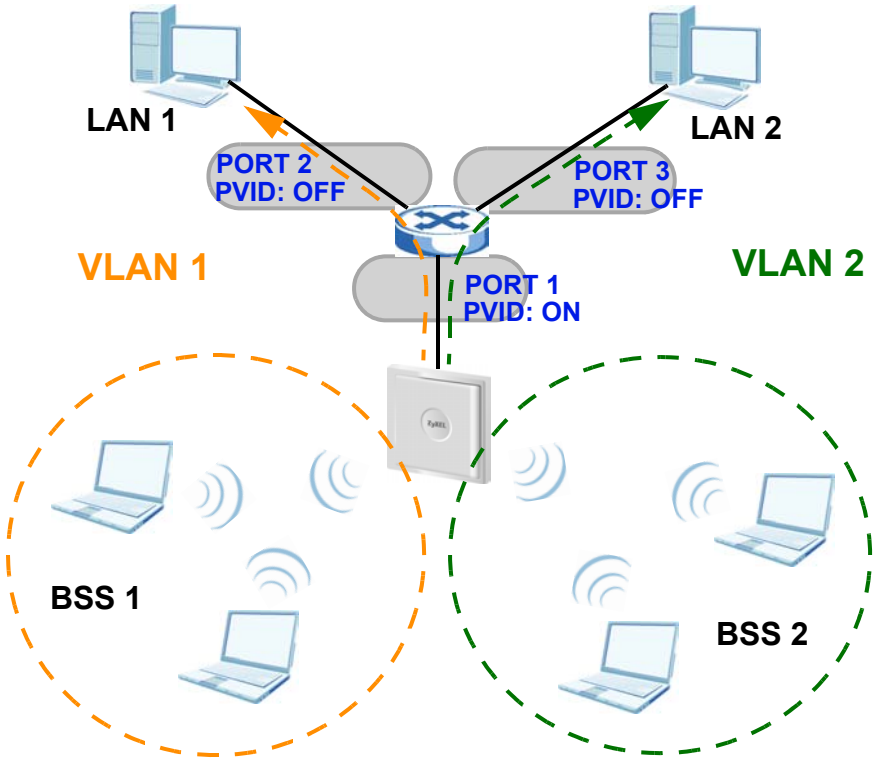
Refer to the applications section for more information.

9.1.4 Multiple BSS with VLAN Example

In this example, **VLAN 1** includes the computers in **BSS1** and **LAN 1**. Computers in **BSS2** and **LAN 2** belong to **VLAN 2**. Users in **BSS1** are limited to accessing the resources on **LAN 1** and similarly users in **BSS2** may only access resources on **LAN 2**. **VLAN 2** is the management VLAN.

The switch adds PVID (Port VLAN IDentity) tags to incoming frames that don't already have tags (on switch ports where PVID is enabled).

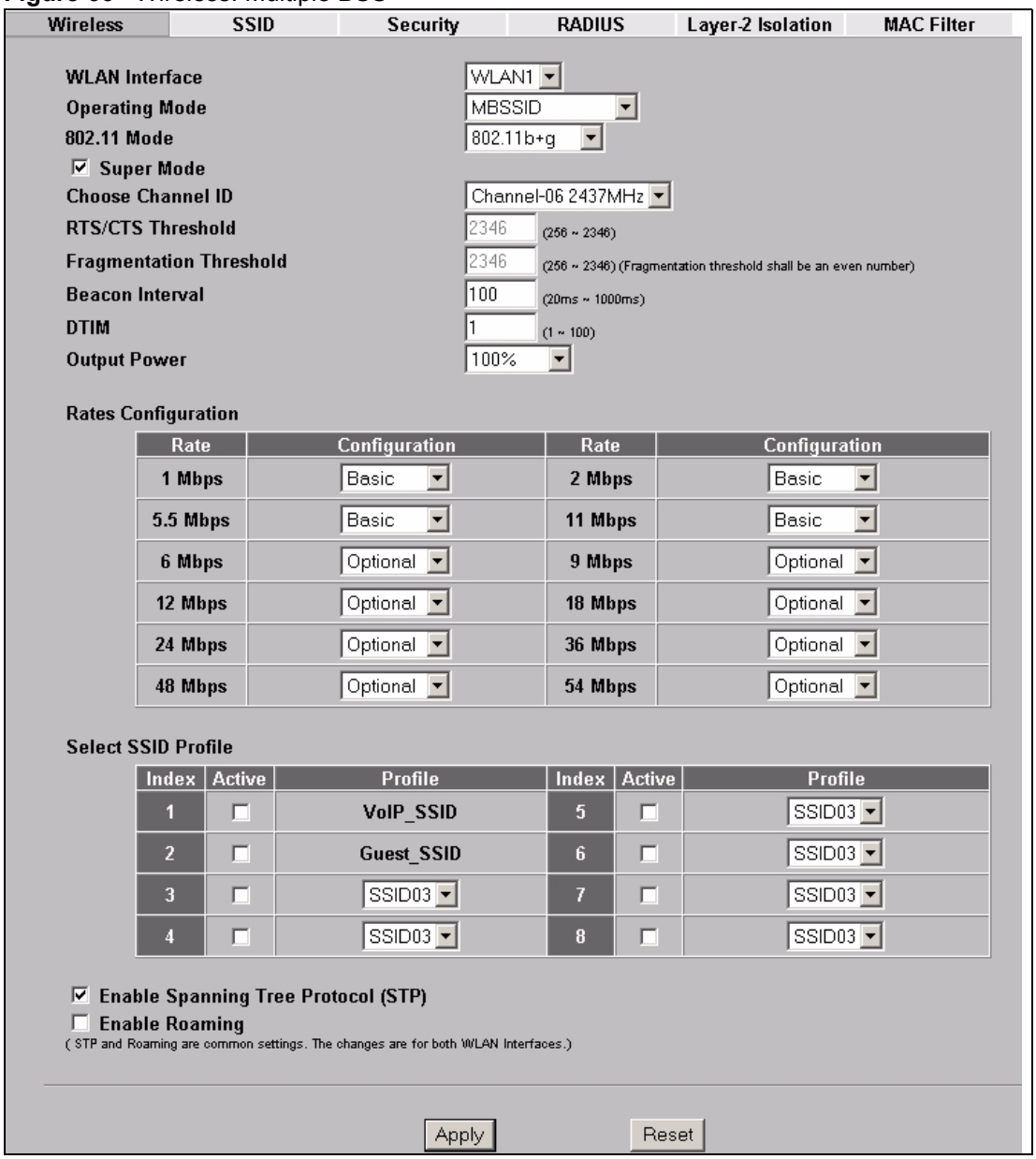
Figure 65 Multiple BSS with VLAN Example



9.1.5 Configuring Multiple BSSs

Click **WIRELESS** > **Wireless** and select **MBSSID** in the **Operating Mode** drop-down list box to display the screen as shown.

Figure 66 Wireless: Multiple BSS



The following table describes the labels in this screen.

Table 34 Wireless: Multiple BSS

LABEL	DESCRIPTION
WLAN Interface	Select which WLAN adapter you want to configure. It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.
Operating Mode	Select **MBSSID** in this field to display the screen as shown

Table 34 Wireless: Multiple BSS

LABEL	DESCRIPTION
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11a** to allow only IEEE 802.11a compliant WLAN devices to associate with the ZyXEL Device.
Super Mode	Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyXEL Device automatically select a channel, click **Scan** instead.
Scan	Click this button to have the ZyXEL Device automatically select the wireless channel with the lowest interference.
Disable channel switching for DFS	This field is available when you select **802.11a** in the **802.11 Mode** field. DFS (dynamic frequency selection) allows an AP to detect other devices in the same channel. If there is another device using the same channel, the AP changes to a different channel, so that it can avoid interference with radar systems or other wireless networks. Select this option to disable DFS on the ZyXEL Device when **802.11 Mode** is set to **802.11a**.
RTS/CTS Threshold	The threshold (number of bytes) for enabling RTS/CTS handshake. Data with a frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its lowest value (256) turns on the RTS/CTS handshake. Enter a value between **256** and **2346**. This field is not available when **Super Mode** is selected.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**. This field is not available when **Super Mode** is selected.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following **100%**, **50%**, **25%**, **12.5%** or **Minimum**. See the product specifications for more information on your ZyXEL Device's output power. This field is not available when you select **802.11a** in the **802.11 Mode** field.
Rates Configuration	This section controls the data rates permitted for clients. For each **Rate**, select an option from the **Configuration** list. The options are: • **Basic** (1~11 Mbps only): Clients can always connect to the access point at this speed. • **Optional**: Clients can connect to the access point at this speed, when permitted to do so by the AP. • **Disabled**: Clients cannot connect to the access point at this speed.

Table 34 Wireless: Multiple BSS

LABEL	DESCRIPTION
Select SSID Profile	An SSID profile is the set of parameters relating to one of the ZyXEL Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating with the access point (AP) must have the same SSID. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Index	This is the index number of the SSID profile.
Active	Select the check box to activate an SSID profile.
Profile	Select the profile(s) of the SSIDs you want to use in your wireless network. You can have up to eight BSSs running on the ZyXEL Device simultaneously, one of which is always the pre-configured **VoIP_SSID** profile and another of which is always the pre-configured **Guest_SSID** profile. Configure SSID profiles in the **SSID** screen.
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.
Enable Roaming	Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this checkbox to enable roaming on the ZyXEL Device if you have two or more ZyXEL Devices on the same subnet. Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

9.2 SSID

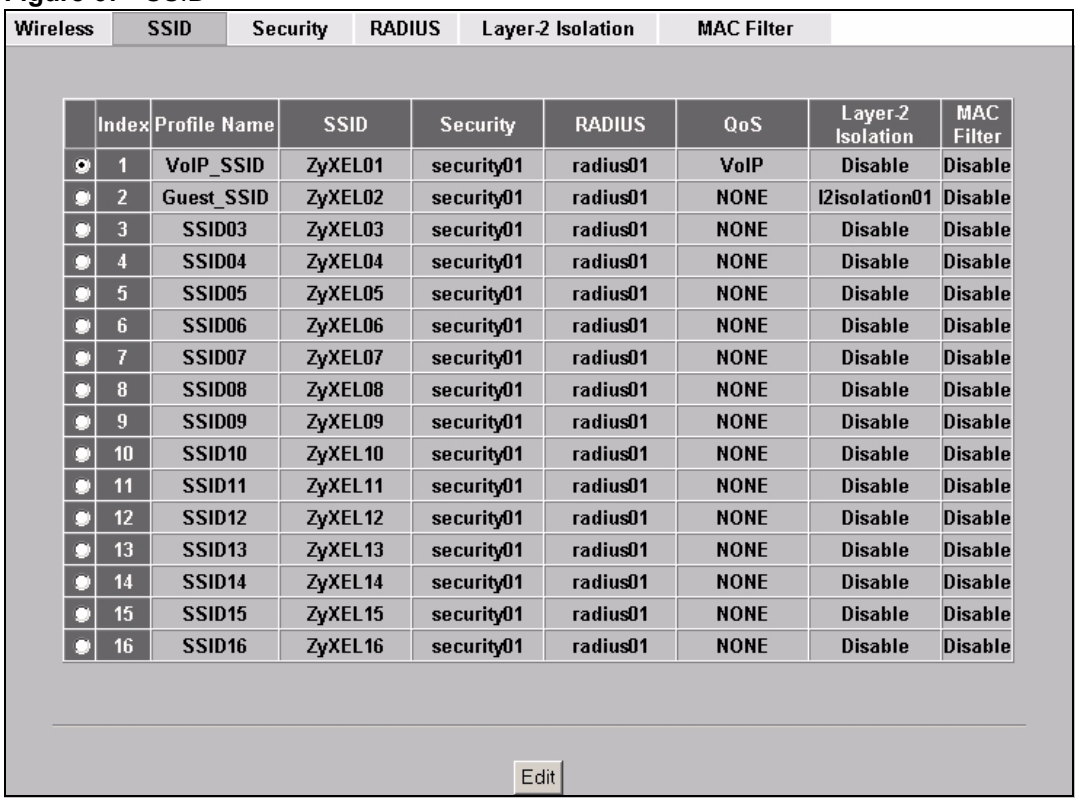
When the ZyXEL Device is set to Access Point, AP+Bridge or MBSSID mode, you need to choose the SSID profile(s) you want to use in your wireless network (see Section 7.6 on page 98 for more information on operating modes).

Use the **WIRELESS** > **SSID** screen to see information about the SSID profiles on the ZyXEL Device, and use the **WIRELESS** > **SSID** > **Edit** screen to configure the SSID profiles.

9.2.1 The SSID Screen

Click **WIRELESS** > **SSID** to display the screen as shown.

Figure 67 SSID



	Index	Profile Name	SSID	Security	RADIUS	QoS	Layer-2 Isolation	MAC Filter
◉	1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
○	2	Guest_SSID	ZyXEL02	security01	radius01	NONE	l2isolation01	Disable
○	3	SSID03	ZyXEL03	security01	radius01	NONE	Disable	Disable
○	4	SSID04	ZyXEL04	security01	radius01	NONE	Disable	Disable
○	5	SSID05	ZyXEL05	security01	radius01	NONE	Disable	Disable
○	6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
○	7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable
○	8	SSID08	ZyXEL08	security01	radius01	NONE	Disable	Disable
○	9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable
○	10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable
○	11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable
○	12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable
○	13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable
○	14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable
○	15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable
○	16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable

Edit

The following table describes the labels in this screen.

Table 35 SSID

LABEL	DESCRIPTION
Index	This field displays the index number of each SSID profile.
Name	This field displays the identification name of each SSID profile on the ZyXEL Device.
SSID	This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates which security profile is currently associated with each SSID profile. See Section 8.3 on page 111 for more information.
RADIUS	This field displays which RADIUS profile is currently associated with each SSID profile, if you have a RADIUS server configured.
QoS	This field displays the Quality of Service setting for this profile or **NONE** if QoS is not configured on a profile.
Layer 2 Isolation	This field displays which layer 2 isolation profile is currently associated with each SSID profile, or **Disable** if Layer 2 Isolation is not configured on an SSID profile.
MAC Filter	This field displays which MAC filter profile is currently associated with each SSID profile, or **Disable** if MAC filtering is not configured on an SSID profile.
Edit	Click the radio button next to the profile you want to configure and click **Edit** to go to the SSID configuration screen.

9.2.2 Configuring SSID

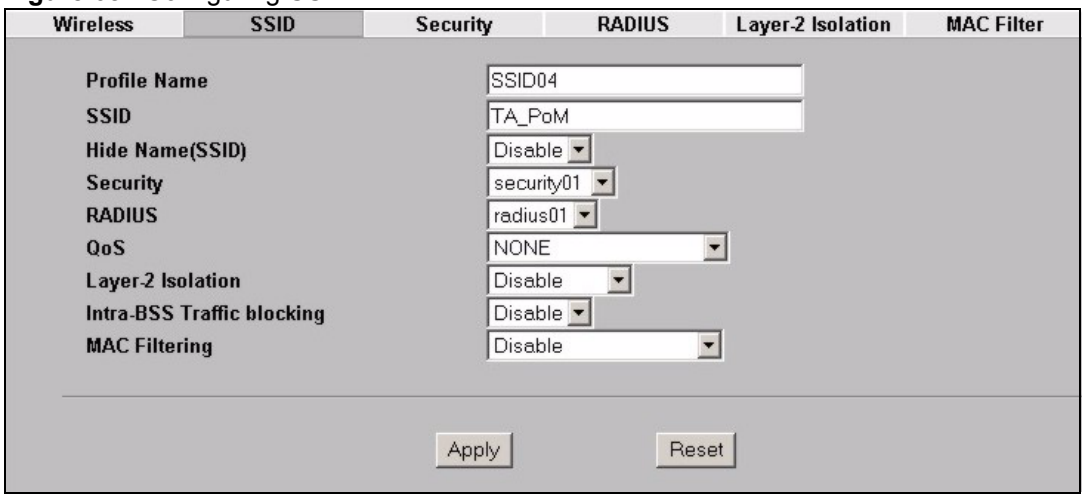
Each SSID profile references the settings configured in the following screens:

- **WIRELESS** > **Security** (one of the security profiles).
- **WIRELESS** > **RADIUS** (one of the RADIUS profiles).
- **WIRELESS** > **MAC Filter** (the MAC filter list, if activated in the SSID profile).
- **WIRELESS** > **Layer 2 Isolation** (the layer 2 isolation list, if activated in the SSID profile).
- Also, use the **VLAN** screen to set up wireless VLANs based on SSID.

Configure the fields in the above screens to use the settings in an SSID profile.

Select an SSID profile in the **WIRELESS** > **SSID** screen and click **Edit** to display the following screen.

Figure 68 Configuring SSID



The following table describes the labels in this screen.

Table 36 Configuring SSID

LABEL	DESCRIPTION
Profile Name	Enter a name identifying this profile.
SSID	When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Hide Name (SSID)	Select **Disable** if you want the ZyXEL Device to broadcast this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, select **Enable** to have the ZyXEL Device hide this SSID (a wireless client scanning for an AP will not find this SSID).
Security	Select a security profile to use with this SSID profile. See Section 8.3 on page 111 for more information.
RADIUS	Select a RADIUS profile from the drop-down list box, if you have a RADIUS server configured. If you do not need to use RADIUS authentication, ignore this field. See Section 8.5 on page 119 for more information.

Table 36 Configuring SSID

LABEL	DESCRIPTION
QoS	Select the Quality of Service priority for this BSS's traffic. • In the pre-configured **VoIP_SSID** profile, the QoS setting is **VoIP**. This is not user-configurable. The **VoIP** setting is available only on the **VoIP_SSID** profile, and provides the highest level of QoS. • If you select **WMM** from the **QoS** list, the priority of a data packet depends on the packet's IEEE 802.1q or DSCP header. See Section 7.3.1 on page 92 for more information on WMM and WMM priorities. If a packet has no WMM value assigned to it, it is assigned the default priority. • If you select **ATC** from the **QoS** list, the ZyXEL Device automatically assigns priority based on packet size. See Section 7.3.2 on page 93 for more information on ATC. • If you select **ATC+WMM** from the **QoS** list, the ZyXEL Device uses WMM on the wireless network and ATC on the wired network. See Section 7.3.3 on page 94 for more information on ATC+WMM. • If you select **WMM_VOICE**, **WMM_VIDEO**, **WMM_BEST_EFFORT** or **WMM_BACKGROUND**, the ZyXEL Device applies that QoS setting to all of that SSID's traffic. • If you select **NONE**, the ZyXEL Device applies no priority to traffic on this SSID. Note: When you configure an SSID profile's QoS settings, the ZyXEL Device applies the same QoS setting to all of the profile's traffic.
Layer-2 Isolation	Select a layer 2 isolation profile from the drop-down list box. If you do not want to use layer 2 isolation on this profile, select **Disable**. See Section 10.1 on page 129 for more information.
Intra-BSS Traffic blocking	Select **Enable** from the drop-down list box to prevent wireless clients in this profile's BSS from communicating with one another.
MAC Filtering	Select a MAC filter profile from the drop-down list box. If you do not want to use MAC filtering on this profile, select **Disable**. See Section 10.4 on page 134 for more information.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

10

Other Wireless Configuration

This chapter describes how to configure the **Layer-2 Isolation** and **MAC Filter** screens on your ZyXEL Device.

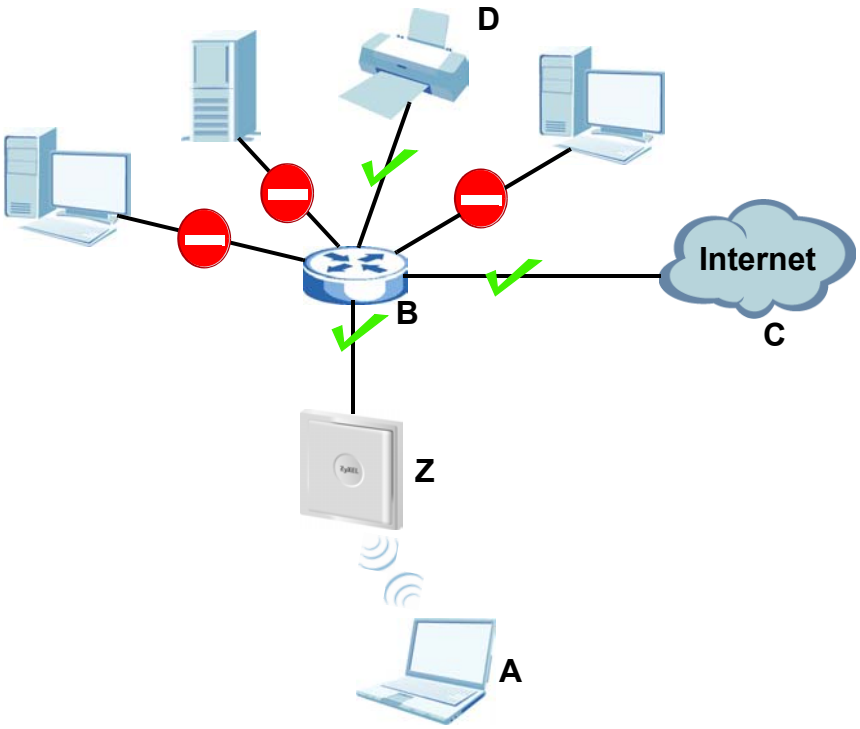
10.1 Layer-2 Isolation Introduction

Layer-2 isolation is used to prevent wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.

In the following example, layer-2 isolation is enabled on the ZyXEL Device (**Z**, in the figure) to allow a guest wireless client (**A**) to access the main network router (**B**). The router provides access to the Internet (**C**) and the network printer (**D**) while preventing the client from accessing other computers and servers on the network. The client can communicate with other wireless clients only if **Intra-BSS Traffic blocking** is disabled.

Intra-BSS Traffic Blocking is activated when you enable layer-2 isolation.

Figure 69 Layer-2 Isolation Application

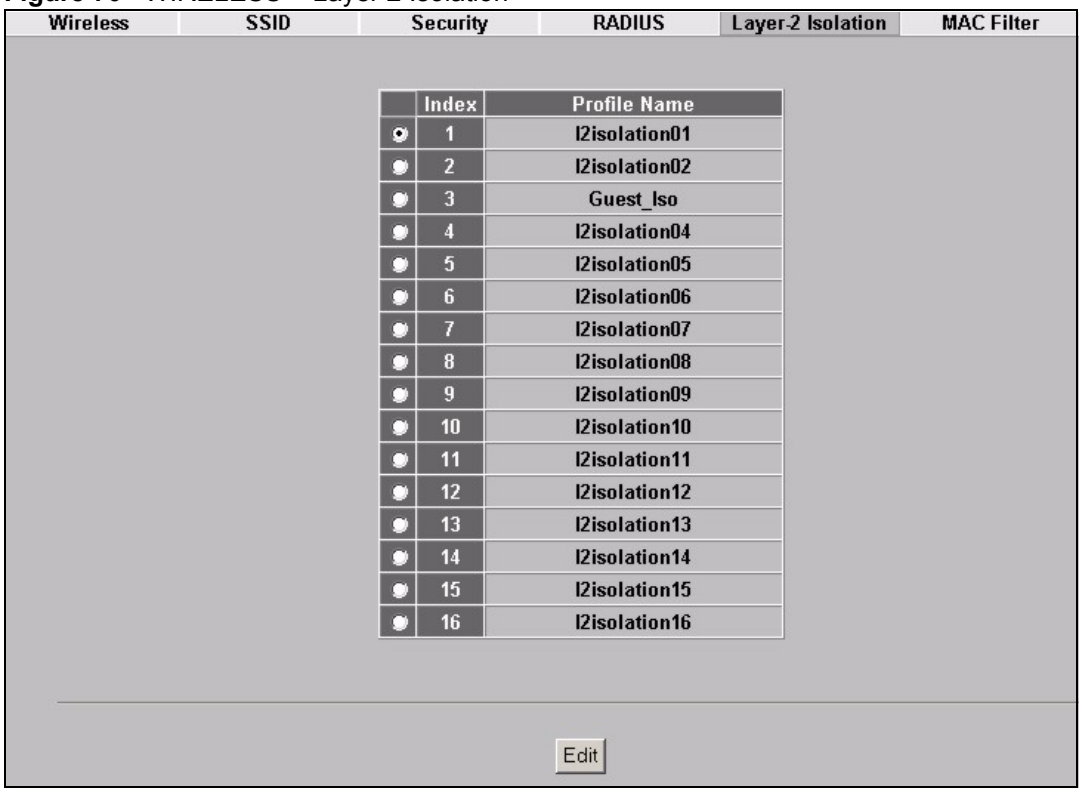


MAC addresses that are not listed in the **Allow devices with these MAC addresses** table are blocked from communicating with the ZyXEL Device's wireless clients except for broadcast packets. Layer-2 isolation does not check the traffic between wireless clients that are associated with the same AP. Intra-BSS Traffic allows wireless clients associated with the same AP to communicate with each other.

10.2 The Layer-2 Isolation Screen

Click **WIRELESS** > **Layer-2 Isolation**. The screen appears as shown next.

Figure 70 WIRELESS > Layer 2 Isolation



The following table describes the labels in this screen.

Table 37 WIRELESS > Layer-2 Isolation

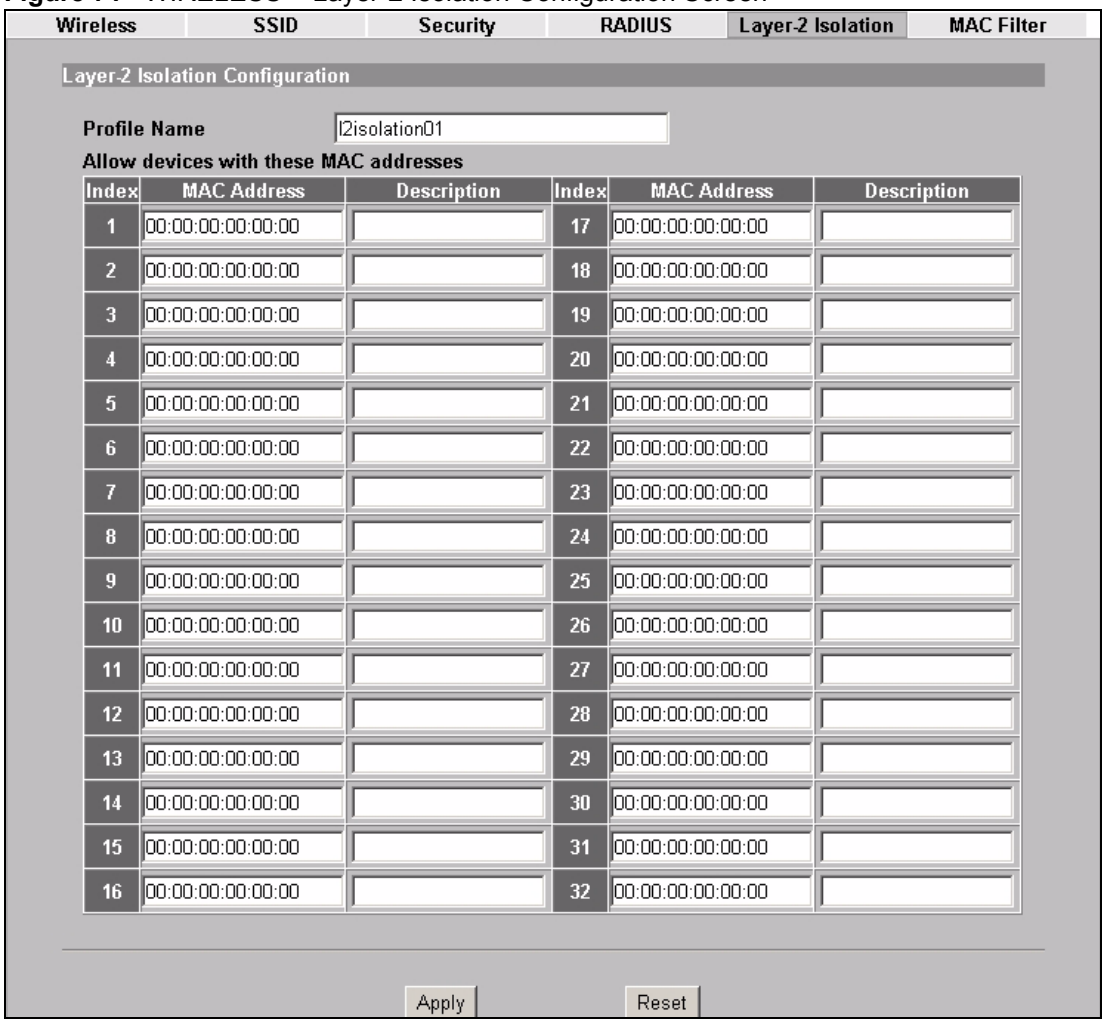
LABEL	DESCRIPTION
Index	This is the index number of the profile.
Profile Name	This field displays the name given to a layer-2 isolation profile in the **Layer-2 Isolation Configuration** screen.
Edit	Select an entry from the list and click **Edit** to configure settings for that profile.

10.3 Configuring Layer-2 Isolation

To configure layer-2 isolation, click **WIRELESS** > **Layer-2 Isolation** > **Edit**. The screen appears as shown.

If layer-2 isolation is enabled, you need to know the MAC address of each wireless client, AP, computer or router that you want to allow to communicate with the ZyXEL Device's wireless clients.

Figure 71 WIRELESS > Layer-2 Isolation Configuration Screen



The following table describes the labels in this screen.

Table 38 WIRELESS > Layer-2 Isolation Configuration

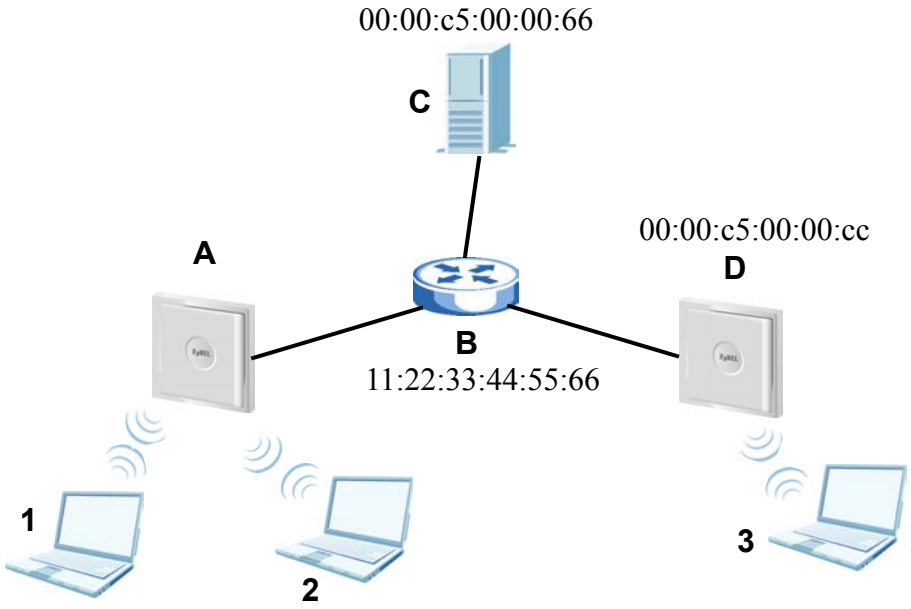
LABEL	DESCRIPTION
Profile Name	Type a name to identify this layer-2 isolation profile.
Allow devices with these MAC addresses	These are the MAC address of a wireless client, AP, computer or router. A wireless client associated with the ZyXEL Device can communicate with another wireless client, AP, computer or router only if the MAC addresses of those devices are listed in this table.
Index	This is the index number of the MAC address.
MAC Address	Type the MAC addresses of the wireless client, AP, computer or router that you want to allow the associated wireless clients to have access to in these address fields. Type the MAC address in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).
Description	Type a name to identify this device.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

10.3.1 Layer-2 Isolation Examples

The following section shows you example layer-2 isolation configurations on the ZyXEL Device (**A**).

When configuring, remember to select the correct layer-2 isolation profile in the **WIRELESS > SSID > Edit** screen of the relevant SSID profile.

Figure 72 Layer-2 Isolation Example Configuration

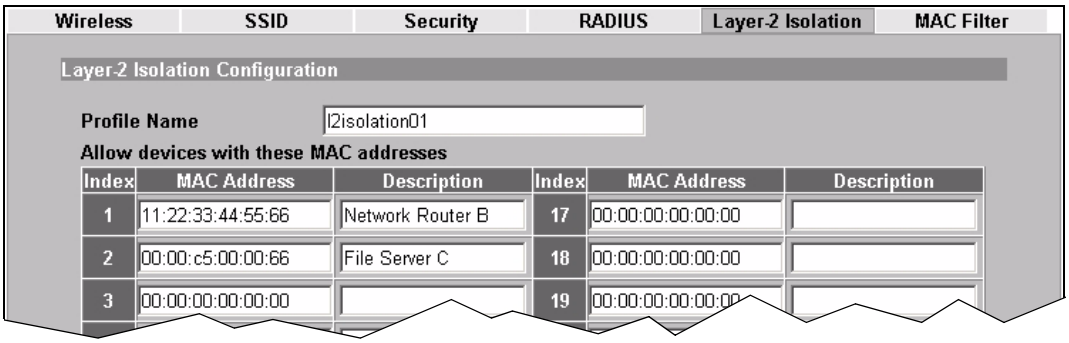


10.3.1.1 Layer-2 Isolation Example 1

In the following example wireless clients **1** and **2** can communicate with network router **B** and file server **C**, but not access point **D** or wireless client **3**.

- Enter **B**'s MAC address in the **MAC Address** field, and enter "Network Router B" in **B**'s **Description** field. Enter **C**'s MAC address in the **MAC Address** field, and enter "File Server C" in **C**'s **Description** field.

Figure 73 Layer-2 Isolation Example 1

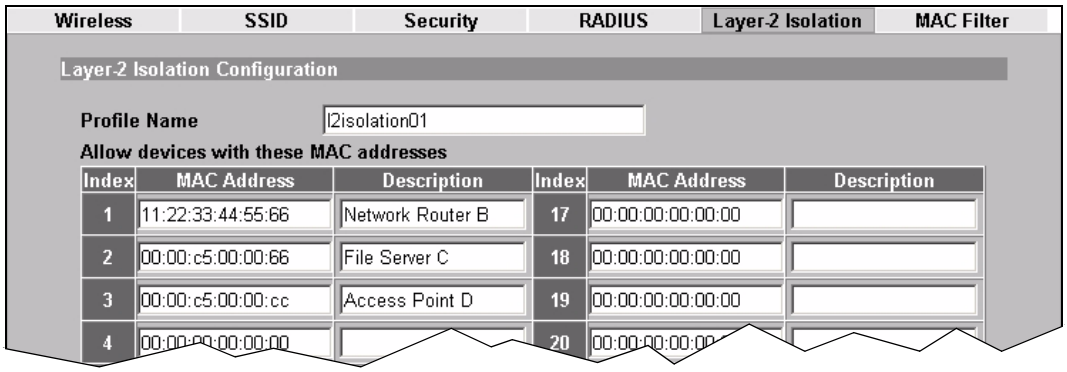


10.3.1.2 Layer-2 Isolation Example 2

In the following example wireless clients **1** and **2** can communicate with access point **D** and file server **C** but not wireless client **3**.

- Enter the router's, server's and access point **D**'s MAC addresses in the **MAC Address** fields. Enter "Network Router B" in **B**'s **Description** field, enter "File Server C" in **C**'s **Description** field, and enter "Access Point D" in **D**'s **Description** field.

Figure 74 Layer-2 Isolation Example 2



10.4 The MAC Filter Screen

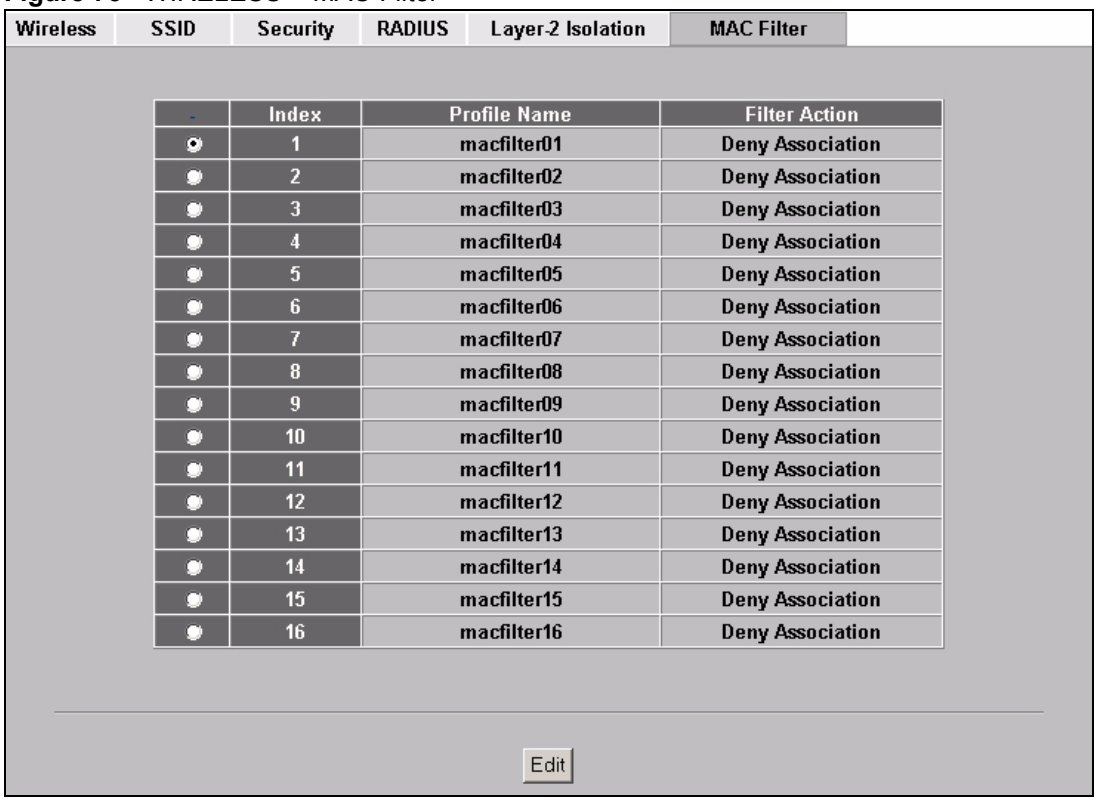
The MAC filter function allows you to configure the ZyXEL Device to give exclusive access to devices (**Allow Association**) or exclude devices from accessing the ZyXEL Device (**Deny Association**).

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of each device to configure MAC filtering on the ZyXEL Device.

The MAC filter profile is a user-configured list of MAC addresses. Each SSID profile can reference one MAC filter profile. The ZyXEL Device provides 16 MAC Filter profiles, each of which can hold up to 32 MAC addresses.

Click **WIRELESS > MAC Filter**. The screen displays as shown.

Figure 75 WIRELESS > MAC Filter



The following table describes the labels in this screen.

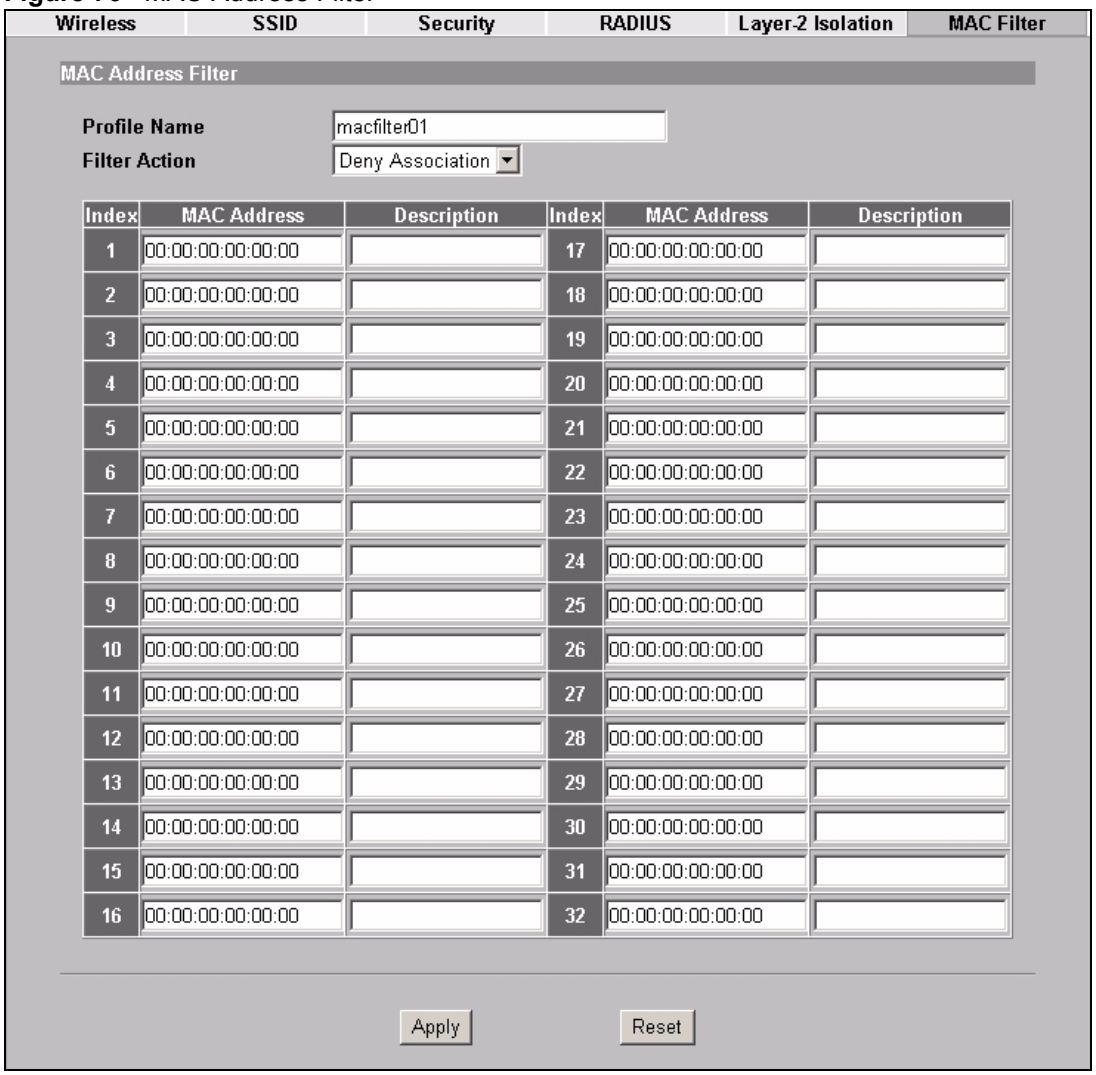
Table 39 WIRELESS > MAC Filter

LABEL	DESCRIPTION
Index	This is the index number of the profile.
Profile Name	This field displays the name given to a MAC filter profile in the **MAC Filter Configuration** screen.
Filter Action	This is the filter action for the list of MAC addresses in the profile.
Edit	Select an entry from the list and click **Edit** to configure settings for that profile.

10.4.1 Configuring MAC Filtering

To change your ZyXEL Device's MAC filter settings, click **WIRELESS** > **MAC Filter** > **Edit**. The screen appears as shown.

Figure 76 MAC Address Filter



The following table describes the labels in this screen.

Table 40 MAC Address Filter

LABEL	DESCRIPTION
Profile Name	Type a name to identify this profile.
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router. MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router. MAC addresses not listed will be denied access to the router.
Index	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station to be allowed or denied access to the ZyXEL Device.
Description	Type a name to identify this wireless station.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

To activate MAC filtering on an SSID profile, select the correct filter from the **Enable MAC Filtering** drop-down list box in the **WIRELESS** > **SSID** > **Edit** screen and click **Apply**.

10.5 Configuring Roaming

A wireless station is a device with an IEEE 802.11a/b/g compliant wireless interface. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

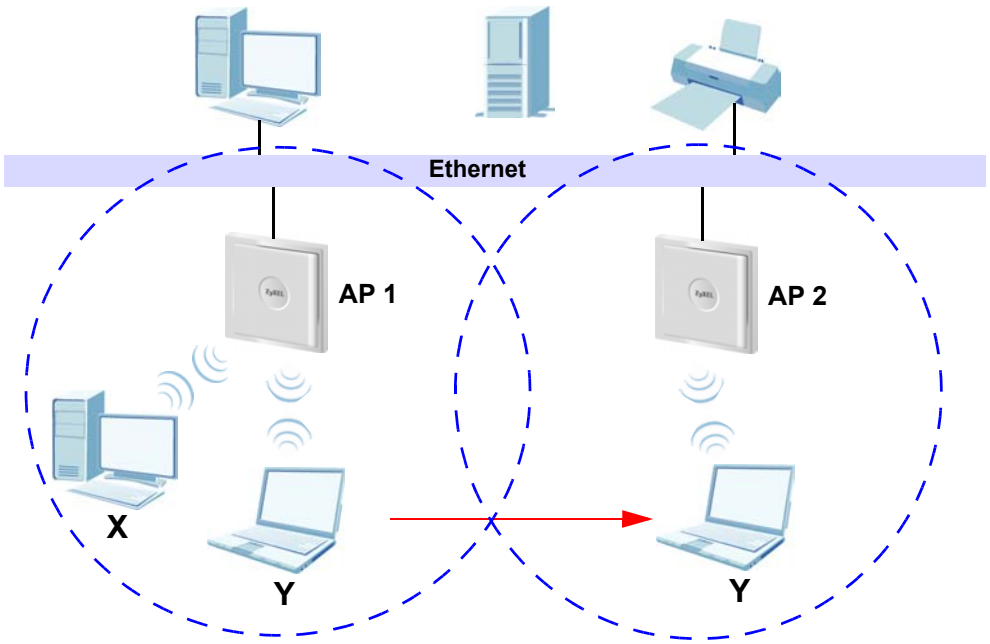
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is known as roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the other access points on the LAN about the change. An example is shown in Figure 77 on page 138.

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this). 802.1x authentication information is not exchanged (at the time of writing).

Figure 77 Roaming Example



The steps below describe the roaming process.

1. Wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**.
2. Wireless station **Y** scans and detects the signal of access point **AP 2**.
3. Wireless station **Y** sends an association request to access point **AP 2**.
4. Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.
5. Access point **AP 1** updates the new position of wireless station **Y**.

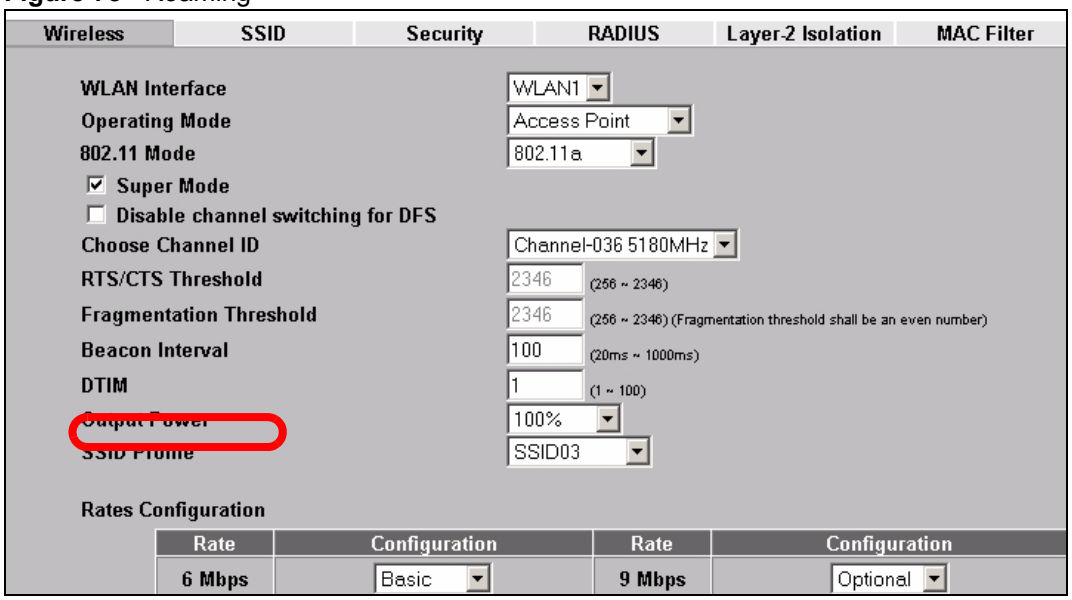
10.5.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3. The adjacent access points should use different radio channels when their coverage areas overlap.
4. All access points must use the same port number to relay roaming information.
5. The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your ZyXEL Device, click **WIRELESS > Wireless**. The screen appears as shown.

Figure 78 Roaming



Select the **Enable Roaming** check box and click **Apply**.

11

IP Screen

This chapter discusses how to configure IP settings on the ZyXEL Device.

11.1 Factory Ethernet Defaults

The Ethernet parameters of the ZyXEL Device are preset in the factory with the following values:

1. IP address of 192.168.1.2
2. Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

11.2 TCP/IP Parameters

11.2.1 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet (only between your two branch offices, for instance) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 41 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

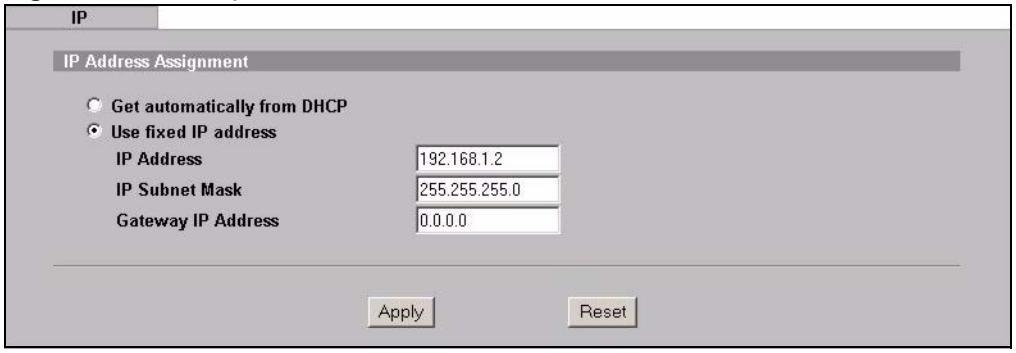
You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

11.3 Configuring IP Settings

Click **IP** to display the screen shown next.

Figure 79 IP Setup



The following table describes the labels in this screen.

Table 42 IP Setup

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option if your ZyXEL Device is using a dynamically assigned IP address from a DHCP server each time. Note: You must know the IP address assigned to the ZyXEL Device (by the DHCP server) to access the ZyXEL Device again.
Use fixed IP address	Select this option if your ZyXEL Device is using a static IP address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Note: If you change the ZyXEL Device's IP address, you must use the new IP address if you want to access the web configurator again.
IP Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the remote nodes.

Table 42 IP Setup

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

12

Rogue AP

This chapter discusses rogue wireless access points (APs) and how to configure the ZyXEL Device's rogue AP detection feature.

12.1 Rogue AP Introduction

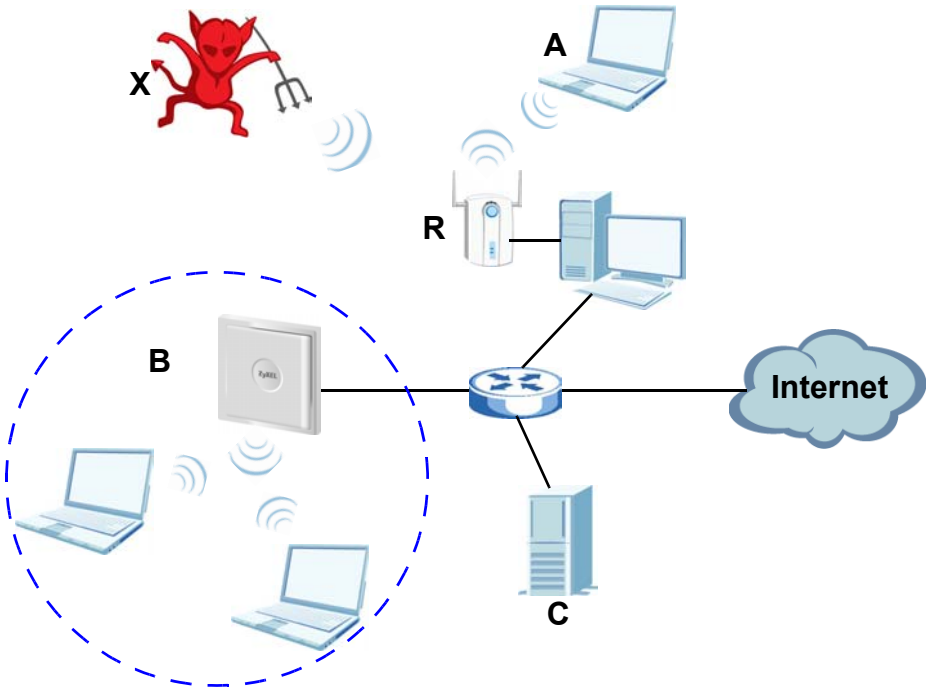
A rogue AP is a wireless access point operating in a network's coverage area that is not a sanctioned part of that network. Rogue APs are not under the control of the network's administrators, and can open up holes in a network's security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain access to the network, or set up their own rogue APs in order to capture information from wireless clients. If a scan reveals a rogue AP, you can use commercially-available software to physically locate it.

Note that it is not necessary for a network to have a legitimate wireless LAN component for rogue APs to open the network to an attacker. In this case, any AP detected can be classified as rogue.

12.2 Rogue AP Examples

In the following example, a corporate network's security is compromised by a rogue AP (**R**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate wireless network (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

Figure 80 Rogue AP: Example



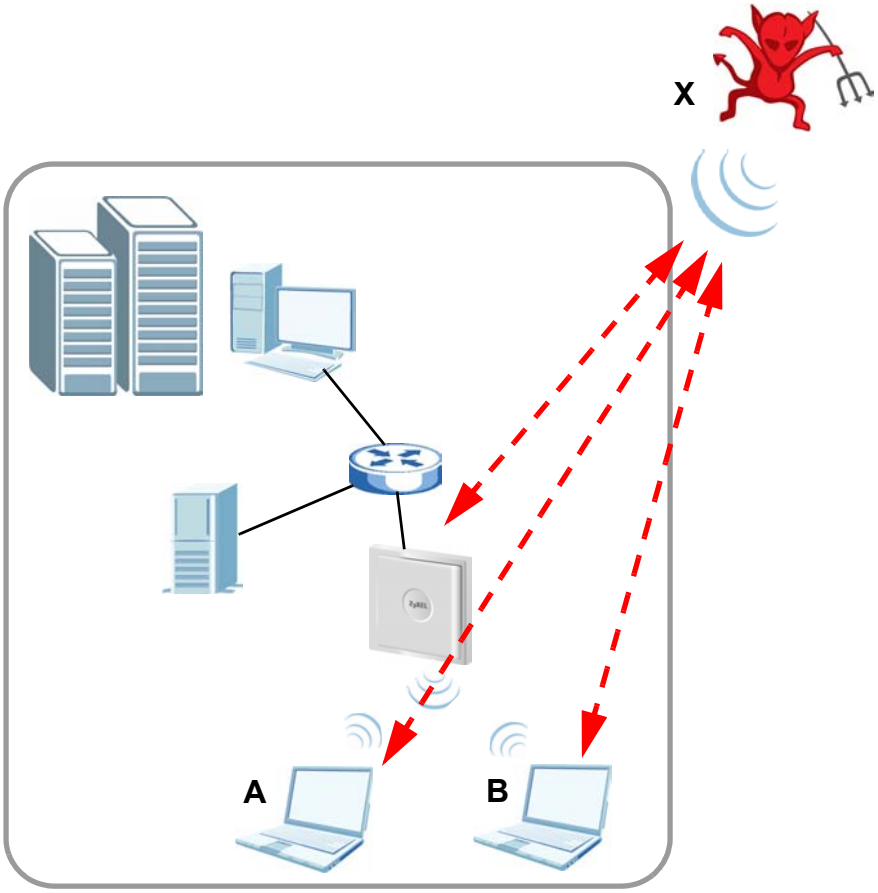
12.2.1 "Honeypot" Attack

Rogue APs need not be connected to the legitimate network to pose a severe security threat. In the following example, an attacker (**X**) is stationed in a vehicle outside a company building, using a rogue access point equipped with a powerful antenna. By mimicking a legitimate (company network) AP, the attacker tries to capture usernames, passwords, and other sensitive information from unsuspecting clients (**A** and **B**) who attempt to connect. This is known as a "honeypot" attack.

If a rogue AP in this scenario has sufficient power and is broadcasting the correct SSID (Service Set IDentifier) clients have no way of knowing that they are not associating with a legitimate company AP. The attacker can forward network traffic from associated clients to a legitimate AP, creating the impression of normal service. This is a variety of "man-in-the-middle" attack.

This scenario can also be part of a wireless denial of service (DoS) attack, in which associated wireless clients are deprived of network access. Other opportunities for the attacker include the introduction of malware (malicious software) into the network.

Figure 81 "Honeypot" Attack



12.3 Configuring Rogue AP Detection

You can configure the ZyXEL Device to detect rogue IEEE 802.11a (5 GHz) and IEEE 802.11b/g (2.4 GHz) APs.

If you have more than one AP in your wireless network, you must also configure the list of "friendly" APs. Friendly APs are the other wireless access points in your network, as well as any others that you know are not a threat (those from neighboring networks, for example). It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points.

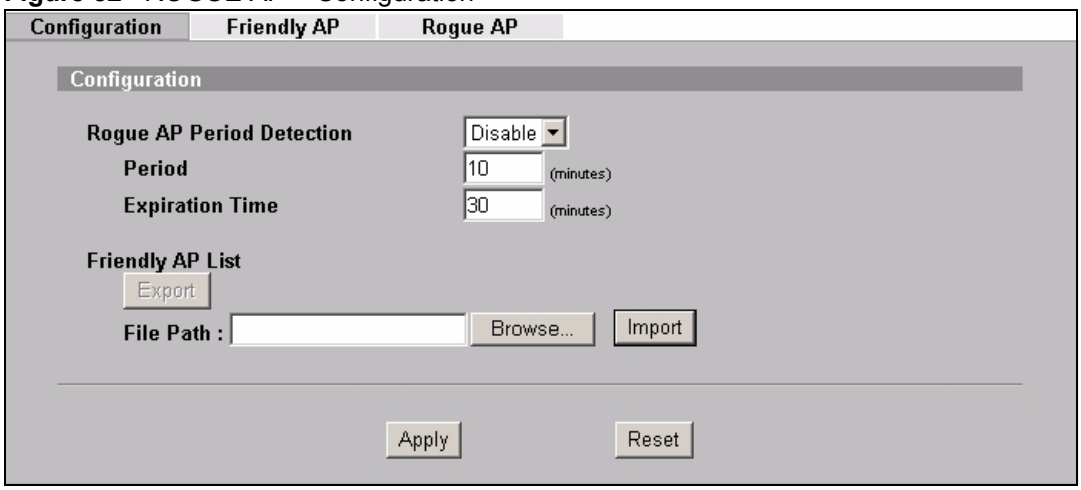
You can choose to scan for rogue APs manually, or to have the ZyXEL Device scan automatically at pre-defined intervals.

You can also set the ZyXEL Device to email you immediately when a rogue AP is detected (see Chapter 16 on page 195 for information on how to set up email logs).

12.3.1 Rogue AP: Configuration

Click **ROGUE AP** > **Configuration**. The following screen appears.

Figure 82 ROGUE AP > Configuration



The following table describes the labels in this screen.

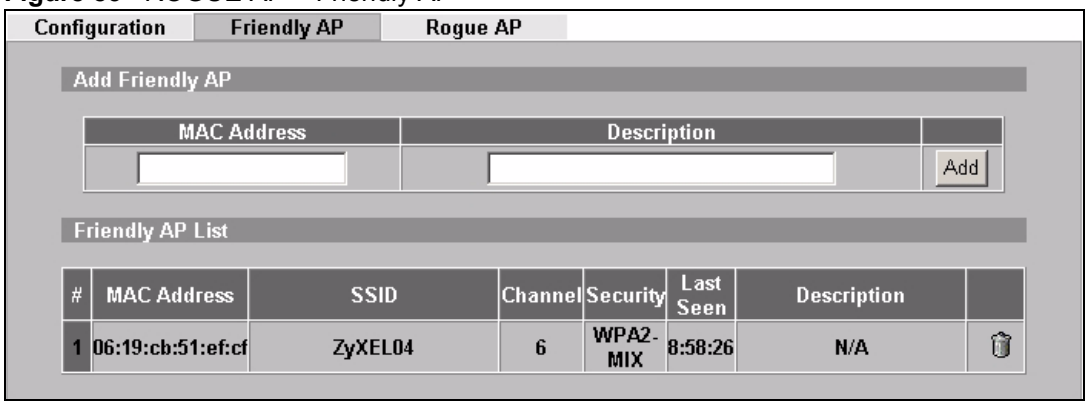
Table 43 ROGUE AP > Configuration

LABEL	DESCRIPTION
Rogue AP Period Detection	Select **Enable** to turn rogue AP detection on. You must also enter a time value in the **Period** field. Select **Disable** to turn rogue AP detection off.
Period (minutes)	Enter the period you want the ZyXEL Device to wait between scanning for rogue APs (between 10 and 60 minutes). You must also select **Enable** in the **Rogue AP Period Detection** field.
Expiration Time (minutes)	Specify how long (between 30 and 180 minutes) an AP's entry can remain in the **Rogue AP List** before the ZyXEL Device removes it from the list if the AP is no longer active.
Friendly AP List	
Export	Click this button to save the current list of friendly APs' MAC addresses and descriptions (as displayed in the **ROGUE AP** > **Friendly AP** screen) to your computer.
File Path	Enter the location of a previously-saved friendly AP list to upload to the ZyXEL Device. Alternatively, click the **Browse** button to locate a list.
Browse	Click this button to locate a previously-saved list of friendly APs to upload to the ZyXEL Device.
Import	Click this button to upload the previously-saved list of friendly APs displayed in the **File Path** field to the ZyXEL Device.
Apply	Click **Apply** to save your settings.
Reset	Click **Reset** to return all fields in this screen to their previously-saved values.

12.3.2 Rogue AP: Friendly AP

The friendly AP list displays details of all the access points in your area that you know are not a threat. If you have more than one AP in your network, you need to configure this list to include your other APs. If your wireless network overlaps with that of a neighbor (for example) you should also add these APs to the list, as they do not compromise your own network's security. If you do not add them to the friendly AP list, these access points will appear in the **Rogue AP** list each time the ZyXEL Device scans.

Figure 83 ROGUE AP > Friendly AP



The following table describes the labels in this screen.

Table 44 ROGUE AP > Friendly AP

LABEL	DESCRIPTION
Add Friendly AP	Use this section to manually add a wireless access point to the list. You must know the device's MAC address.
MAC Address	Enter the MAC address of the AP you wish to add to the list.
Description	Enter a short, explanatory description identifying the AP with a maximum of 32 alphanumeric characters. Spaces, underscores (_) and dashes (-) are allowed.
Add	Click this button to include the AP in the list.
Friendly AP List	This is the list of safe wireless access points you have already configured.
#	This is the index number of the AP's entry in the list.
MAC Address	This field displays the Media Access Control (MAC) address of the AP. All wireless devices have a MAC address that uniquely identifies them.
SSID	This field displays the Service Set IDentifier (also known as the network name) of the AP.
Channel	This field displays the wireless channel the AP is currently using.
Security	This field displays the type of wireless encryption the AP is currently using.
Last Seen	This field displays the last time the ZyXEL Device scanned for the AP.
Description	This is the description you entered when adding the AP to the list.
Delete	Click this button to remove an AP's entry from the list.

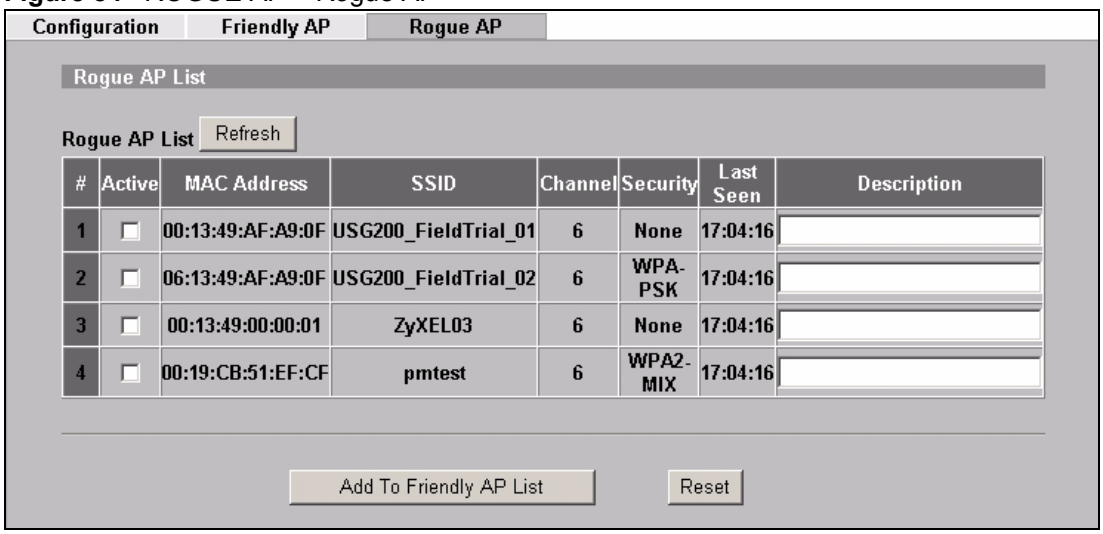
12.3.3 Rogue AP List

This list displays details of all IEEE 802.11a/b/g wireless access points within the ZyXEL Device's coverage area, except for the ZyXEL Device itself and the access points included in the friendly AP list (see Section 12.3.2 on page 148).

You can set how often you want the ZyXEL Device to scan for rogue APs in the **ROGUE AP** > **Configuration** screen (see Section 12.3.1 on page 147).

Click **ROGUE AP** > **Rogue AP**. The following screen displays.

Figure 84 ROGUE AP > Rogue AP



The following table describes the labels in this screen.

Table 45 ROGUE AP > Rogue AP

LABEL	DESCRIPTION
Rogue AP List	This displays details of access points in the ZyXEL Device's coverage area that are not listed in the friendly AP list (see Section 12.3.2 on page 148)
Refresh	Click this button to have the ZyXEL Device scan for rogue APs.
#	This is the index number of the AP's entry in the list.
Active	Use this check box to select the APs you want to move to the friendly AP list (see Section 12.3.2 on page 148).
MAC Address	This field displays the Media Access Control (MAC) address of the AP. All wireless devices have a MAC address that uniquely identifies them.
SSID	This field displays the Service Set IDentifier (also known as the network name) of the AP.
Channel	This field displays the wireless channel the AP is currently using.
Security	This field displays the type of wireless encryption the AP is currently using.
Last Seen	This field displays the last time the ZyXEL Device scanned for the AP.
Description	If you want to move the AP's entry to the friendly AP list, enter a short, explanatory description identifying the AP before you click **Add to Friendly AP List**. A maximum of 32 alphanumeric characters are allowed in this field. Spaces, underscores (_) and dashes (-) are allowed.
Add to Friendly AP List	If you know that the AP described in an entry is not a threat, select the **Active** check box, enter a short description in the **Description** field and click this button to add the entry to the friendly AP list (see Section 12.3.2 on page 148). When the ZyXEL Device next scans for rogue APs, the selected AP does not appear in the rogue AP list.
Reset	Click **Reset** to return all fields in this screen to their default values.

13

Remote Management Screens

This chapter provides information on the Remote Management screens.

13.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

You may manage your ZyXEL Device from a remote location via:

Table 46 Remote Management Overview

- WLAN
- LAN only
- ALL (LAN and WLAN)
- Neither (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Console port
2. SSH
3. Telnet
4. HTTPS and HTTP

13.1.1 Remote Management Limitations

Remote management over LAN or WLAN will not work when:

1. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

13.1.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

13.2 SSH

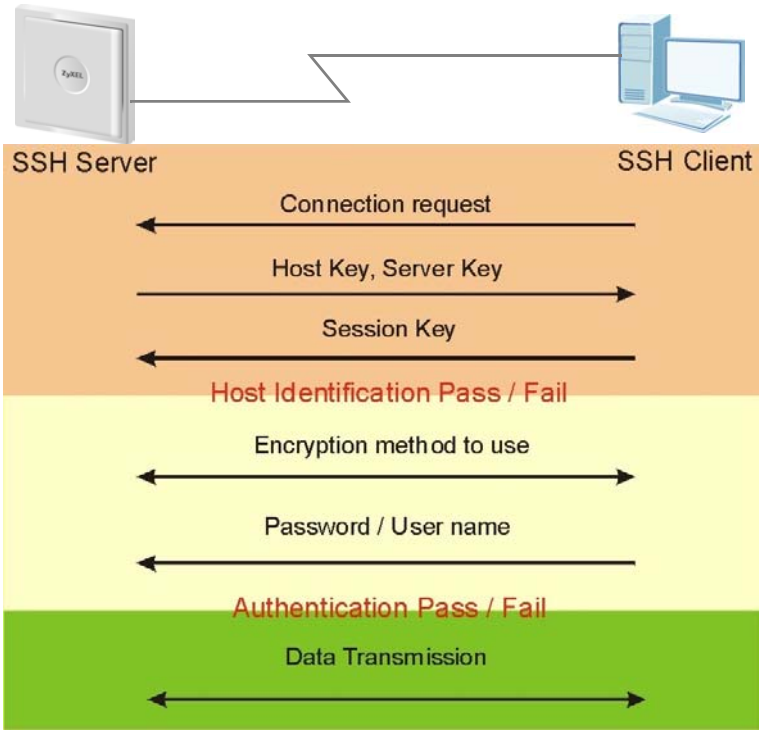
You can use SSH (Secure SHell) to securely access the ZyXEL Device's SMT or command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

13.3 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 85 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

13.4 SSH Implementation on the ZyXEL Device

Your ZyXEL Device supports SSH version 1.0 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyXEL Device for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

13.4.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyXEL Device over SSH.

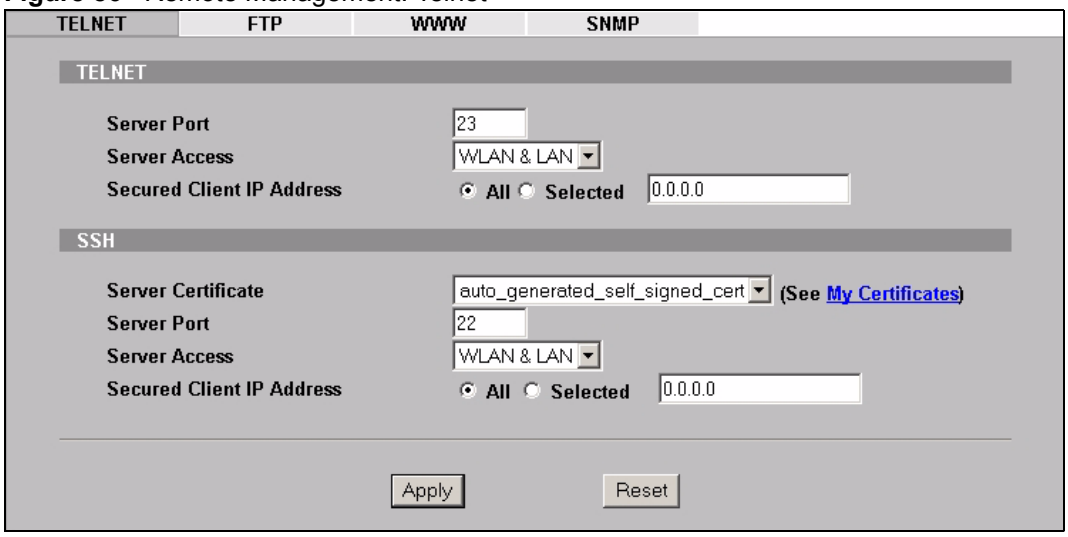
13.5 Configuring Telnet

You can use Telnet to access the ZyXEL Device's SMT or command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click the **REMOTE MGNT** > **TELNET**. The following screen displays.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 86 Remote Management: Telnet



The following table describes the labels in this screen.

Table 47 Remote Management: Telnet

LABEL	DESCRIPTION
TELNET	
Server Port	You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using Telnet.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
SSH	
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the ZyXEL Device for SSH connections. You must have certificates already configured in the **CERTIFICATES** > **My Certificates** screen.
Server Port	You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using SSH.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

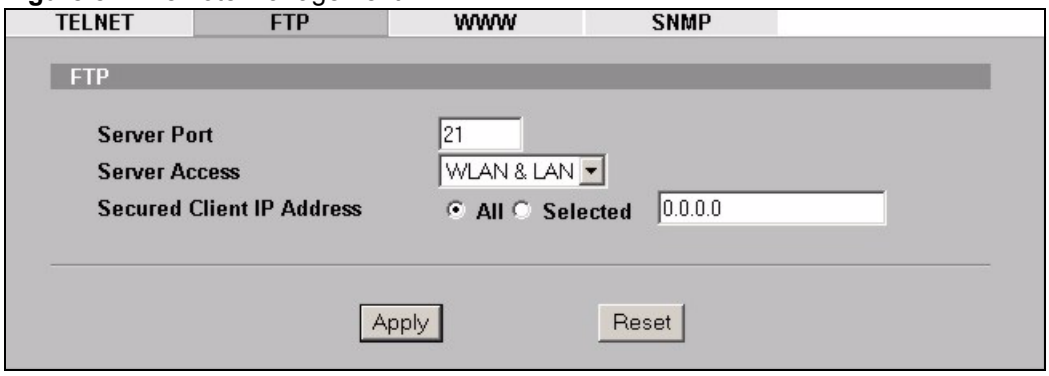
13.6 Configuring FTP

You can use FTP (File Transfer Protocol) to upload and download the ZyXEL Device's firmware and configuration files, please see the User's Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device's FTP settings, click **REMOTE MGNT** > **FTP**.. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 87 Remote Management: FTP



The following table describes the labels in this screen.

Table 48 Remote Management: FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

13.7 WWW (HTTP and HTTPS)

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

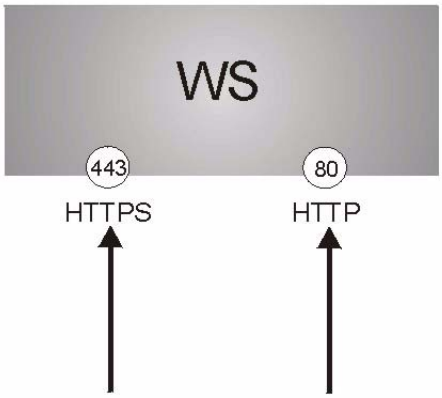
It relies upon certificates, public keys, and private keys (see Chapter 15 on page 177 for more information).

HTTPS on the ZyXEL Device is used so that you may securely access the ZyXEL Device using the web configurator. The SSL protocol specifies that the SSL server (the ZyXEL Device) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT > WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyXEL Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyXEL Device.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyXEL Device's WS (web server).
2. HTTP connection requests from a web browser go to port 80 (by default) on the ZyXEL Device's WS (web server).

Figure 88 HTTPS Implementation

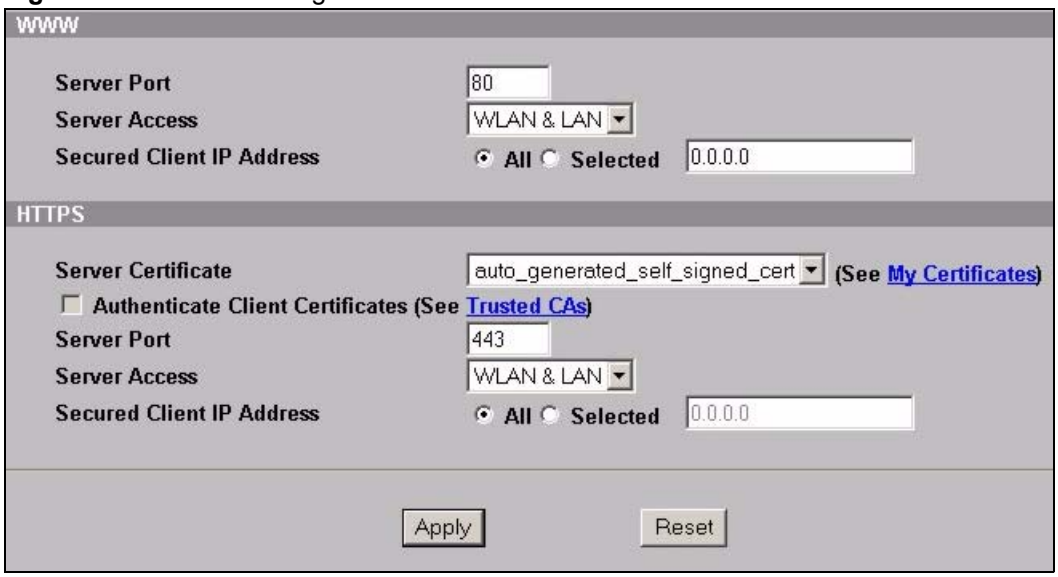


If you disable the **HTTP** service in the **REMOTE MGMT > WWW** screen, then the ZyXEL Device blocks all HTTP connection attempts.

13.8 Configuring WWW

To change your ZyXEL Device's World Wide Web settings, click **REMOTE MGNT** > **WWW**.

Figure 89 Remote Management: WWW



The following table describes the labels in this screen.

Table 49 Remote Management: WWW

LABEL	DESCRIPTION
WWW	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
HTTPS	
Server Certificate	Select the **Server Certificate** that the ZyXEL Device will use to identify itself. The ZyXEL Device is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device).
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself with the ZyXEL Device by sending the ZyXEL Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyXEL Device (see the appendix on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyXEL Device, for example 8443, then you must notify people who need to access the ZyXEL Device web configurator to use "https://ZyXEL Device IP Address:**8443**" as the URL.

Table 49 Remote Management: WWW

LABEL	DESCRIPTION
Server Access	Select a ZyXEL Device interface from **Server Access** on which incoming HTTPS access is allowed. You can allow only secure web configurator access by setting the **WWW Server Access** field to **Disable** and setting the **HTTPS Server Access** field to an interface(s).
Secured Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

13.9 HTTPS Example

If you haven't changed the default HTTPS port on the ZyXEL Device, then in your browser enter "https://ZyXEL Device IP Address/" as the web site address where "ZyXEL Device IP Address" is the IP address or domain name of the ZyXEL Device you wish to access.

13.9.1 Internet Explorer Warning Messages

When you attempt to access the ZyXEL Device HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyXEL Device.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 90 Security Alert Dialog Box (Internet Explorer)

13.9.2 Netscape Navigator Warning Messages

When you attempt to access the ZyXEL Device HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyXEL Device.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyXEL Device's certificate into the SSL client.

Figure 91 Security Certificate 1 (Netscape)

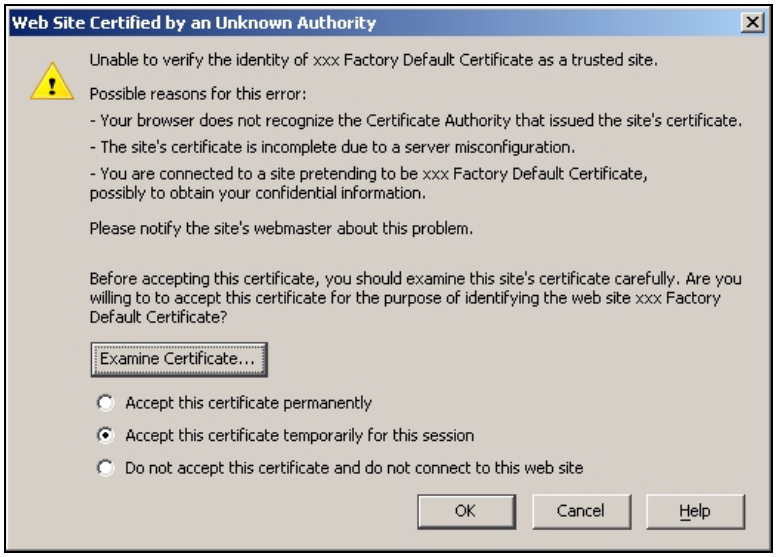
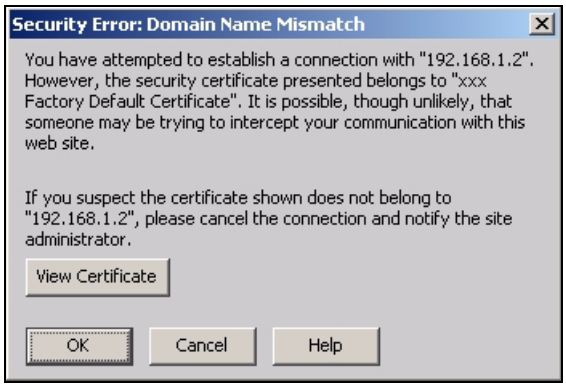


Figure 92 Security Certificate 2 (Netscape)



13.9.3 Avoiding the Browser Warning Messages

The following describes the main reasons that your browser displays warnings about the ZyXEL Device's HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the ZyXEL Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ZyXEL Device's factory default certificate is the ZyXEL Device itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
  - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix D on page 289 for details.
- The actual IP address of the HTTPS server (the IP address of the ZyXEL Device's port that you are trying to access) does not match the common name specified in the ZyXEL Device's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your ZyXEL Device sends to HTTPS clients.

2a Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

2b Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see Figure 95 on page 162 for an example).

Use this procedure to have the ZyXEL Device use a certificate with a common name that matches the ZyXEL Device's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

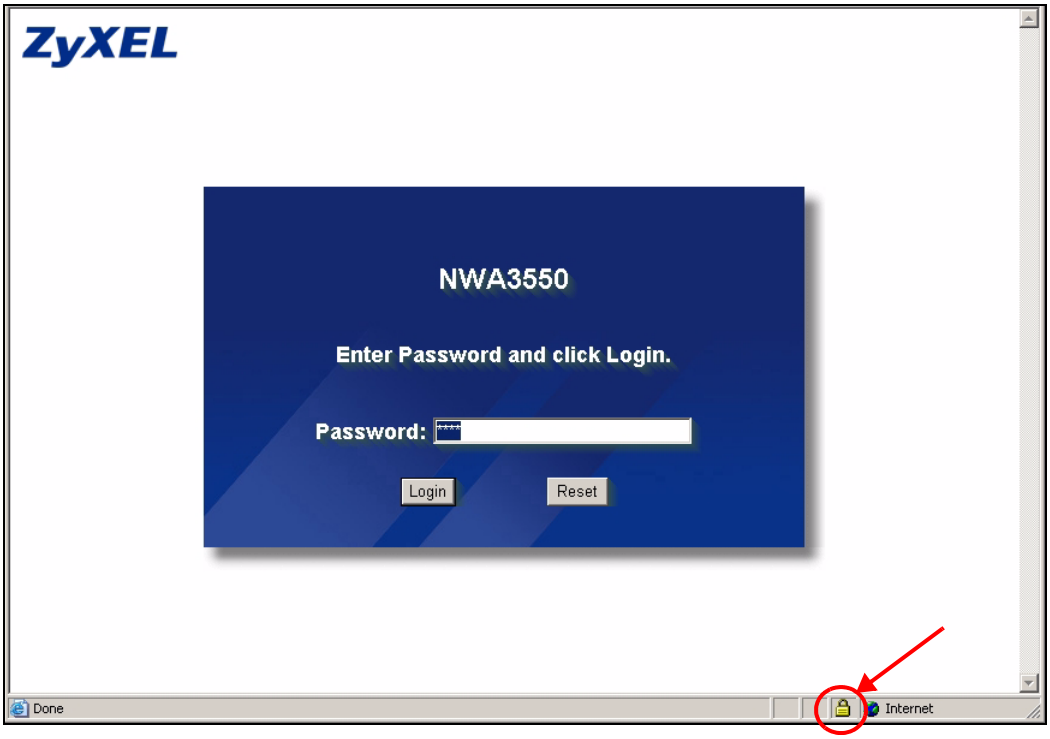
2a Create a new certificate for the ZyXEL Device that uses the IP address (of the ZyXEL Device's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.2, create a certificate that uses 192.168.1.2 as the common name.

2b Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

13.9.4 Login Screen

After you accept the certificate, the ZyXEL Device login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

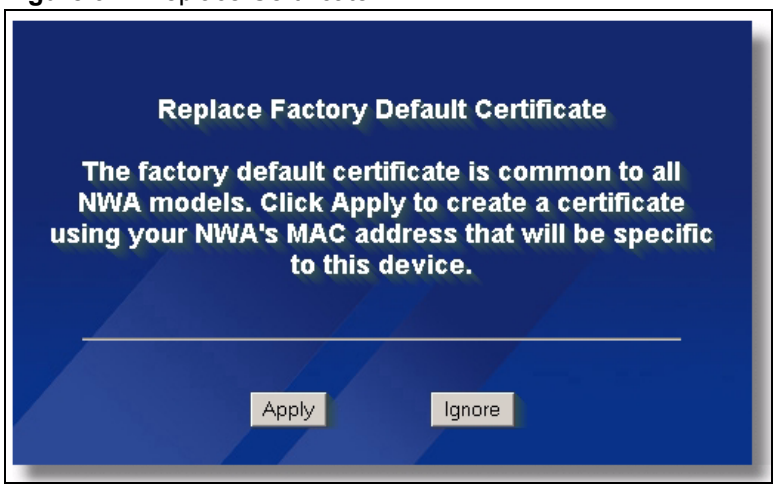
Figure 93 Example: Lock Denoting a Secure Connection



Click **Login** and you then see the next screen.

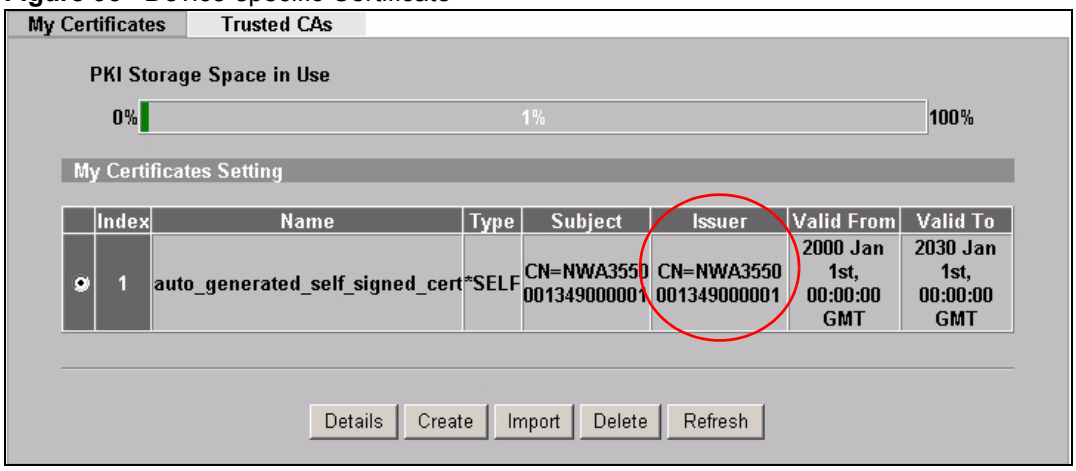
The factory default certificate is a common default certificate for all ZyXEL Device models.

Figure 94 Replace Certificate



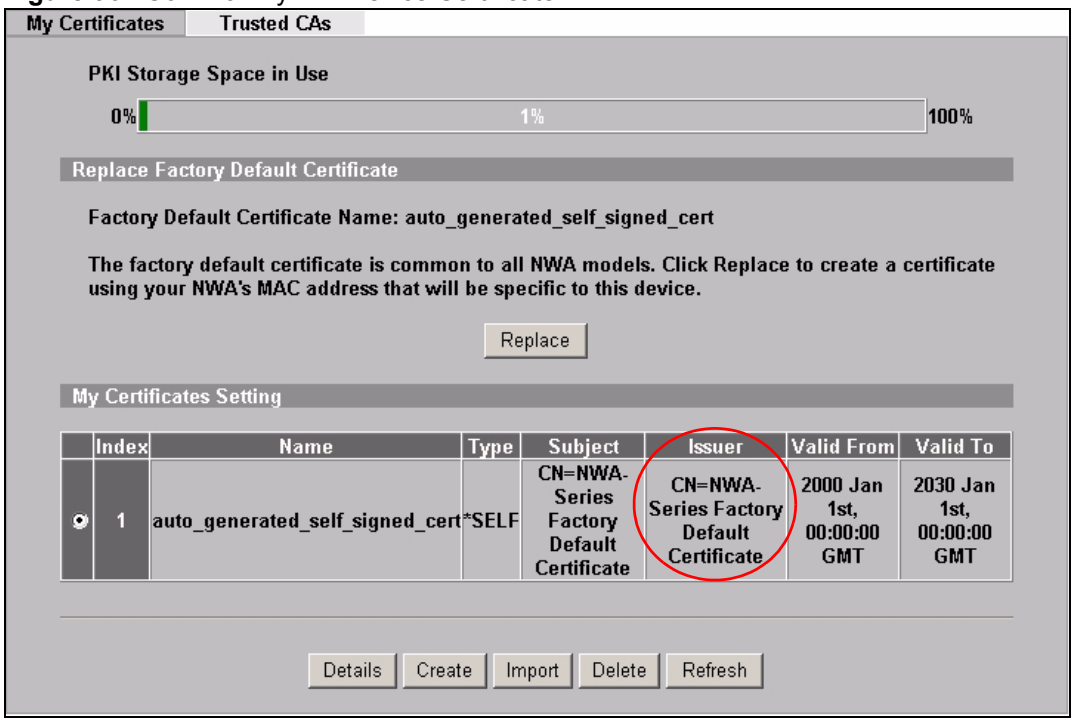
Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

Figure 95 Device-specific Certificate



Click **Ignore** in the **Replace Certificate** screen to use the common ZyXEL Device certificate. You will then see this information in the **My Certificates** screen.

Figure 96 Common ZyXEL Device Certificate

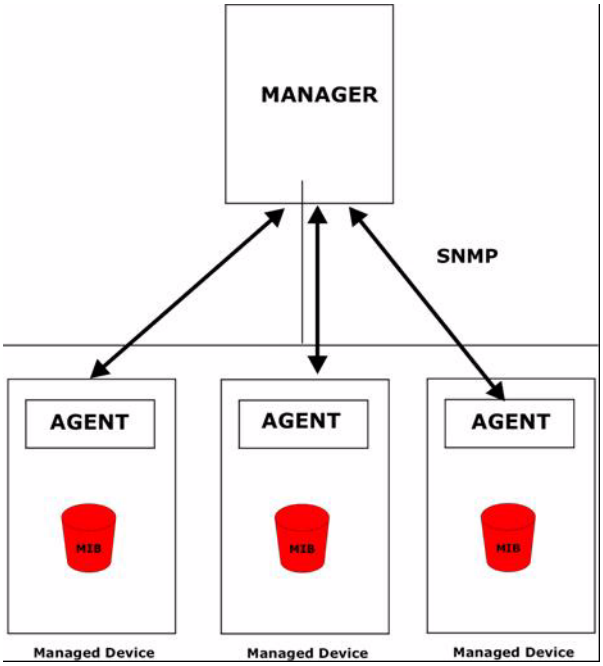


13.10 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1), version two (SNMPv2c), and version 3 (SNMPv3), at the time of writing. The next figure illustrates an SNMP management operation.

SNMP is available only if TCP/IP is configured.

Figure 97 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

13.10.1 Supported MIBs

The ZyXEL Device supports MIB II, which is defined in RFC-1213 and RFC-1215, as well as the proprietary ZyXEL private MIB. The purpose of the MIBs is to let administrators collect statistical data and monitor status and performance.

13.10.2 SNMP Traps

The ZyXEL Device can send the following traps to the SNMP manager.

Table 50 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Generic Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent after booting (power on). This trap is defined in RFC-1215.
warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent after booting (software reboot). This trap is defined in RFC-1215.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure (defined in *RFC-1215*)	1.3.6.1.6.3.1.1.5.5	The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password). Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps.
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.13.0.1	This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.
pwTrapWirelessStatus	1.3.6.1.4.1.890.1.9.2.1.1	This is to enable or disable the wireless group trap.
pwWlanStaAssociation	1.3.6.1.4.1.890.9.2.3.1.1	This trap is sent when a wireless station associates with the ZyXEL Device.
pwWlanStaDisassociation	1.3.6.1.4.1.890.9.2.3.1.2	This trap is sent when a wireless station disconnects from the ZyXEL Device.
pwTrapSecurityStatus	1.3.6.1.4.1.890.1.9.2.1.2	This is to enable or disable the security group trap.
pwWlanStaAuthFail	1.3.6.1.4.1.890.9.2.3.2.1	This trap is sent when a wireless station fails to authenticate with the ZyXEL Device.

Table 50 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
pwTrapTFTPStatus	1.3.6.1.4.1.890.1.9.2.1.3	This is to enable or disable the TFTP group trap.
pwTFTPStatus	1.3.6.1.4.1.890.9.2.3.3.1	This trap is sent to indicate the status and result of a TFTP client session that has ended.

13.11 SNMP Trap Interface Index

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the ZyXEL Device's physical and virtual ports.

Table 51 SNMP Interface Index to Physical and Virtual Port Mapping

TYPE	INTERFACE	PORT
Physical	enet0	Wireless LAN adaptor WLAN1
	enet1	Ethernet port (LAN)
	enet2	Wireless LAN adaptor WLAN2
Virtual	enet3 ~ enet9	WLAN1 in MBSSID mode
	enet10 ~ enet16	WLAN2 in MBSSID mode
	enet17 ~ enet21	WLAN1 in WDS mode
	enet22 ~ enet26	WLAN2 in WDS mode

13.11.1 SNMP v3 and Security

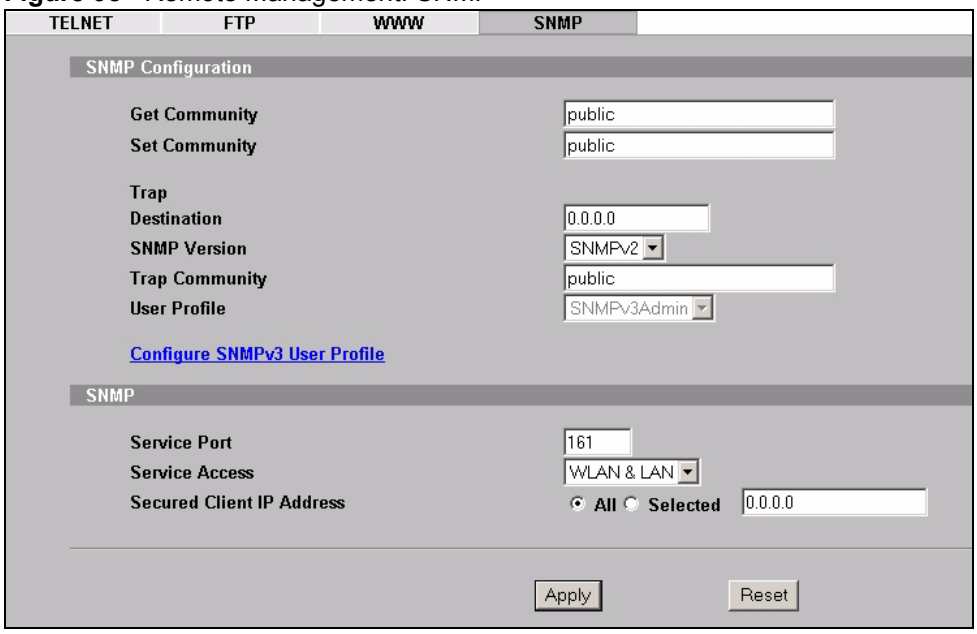
SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

13.11.2 Configuring SNMP

To change your ZyXEL Device's SNMP settings, click **REMOTE MGNT** > **SNMP**. The screen appears as shown.

Figure 98 Remote Management: SNMP



The following table describes the labels in this screen.

Table 52 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set Community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
SNMP Version	Select the SNMP version for the ZyXEL Device. The SNMP version on the ZyXEL Device must match the version on the SNMP manager. Choose SNMP version 1 (**SNMPv1**), SNMP version 2 (**SNMPv2**) or SNMP version 3 (**SNMPv3**).
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is “public” and allows all requests. This field is available only when **SNMPv1** or **SNMPv2** is selected in the **SNMP Version** field.
User Profile	This field is available only when you select **SNMPv3** in the **SNMP Version** field. When sending SNMP v3 traps (messages sent independently by the SNMP agent) the agent must authenticate the SNMP manager. If the SNMP manager does not provide the correct security details, the agent does not send the traps. The ZyXEL Device has two SNMP version 3 login accounts, **User** and **Admin**. Each account has different security settings. You can use either account’s security settings for authenticating SNMP traps. Select **User** to have the ZyXEL Device use the **User** account’s security settings, or select **Admin** to have the ZyXEL Device use the **Admin** account’s security settings. Use the **Configure SNNMPv3 User Profile** link to set up each account’s security settings.
Configure SNMPv3 User Profile	Click this to go to the **SNMPv3 User Profile** screen, where you can configure administration and user login details.

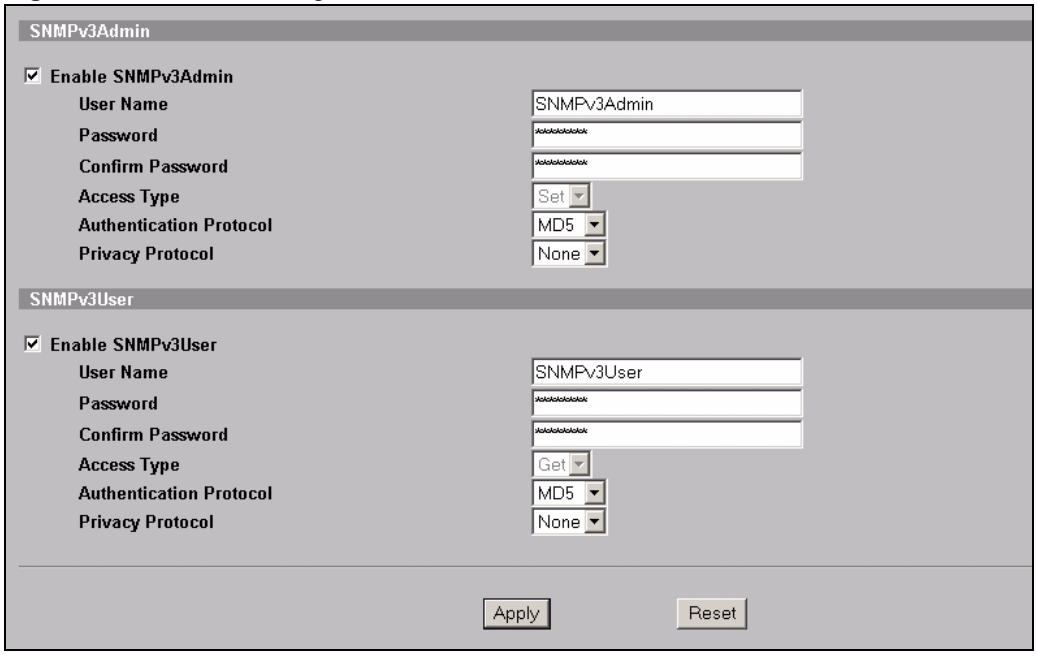
Table 52 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

13.11.2.1 The SNMPv3 User Profile Screen

Use this screen to set up the details of SNMPv3 users. Click **Configure SNMPv3 User Profile** in the **REMOTE MGNT** > **SNMP** screen. The following screen displays.

Figure 99 Remote Management: SNMPv3 User Profile



The following table describes the labels in this screen.

Table 53 Remote Management: SNMP User Profile

LABEL	DESCRIPTION
Enable SNMPv3Admin	Select this box to activate the SNMPv3 administration account. The SNMPv3 administrator can issue Get and Set commands to the ZyXEL Device.
User Name	Enter a username for the SNMPv3 administrator. Only SNMP commands carrying this username are allowed to administer the ZyXEL Device.
Password	Enter a password for the SNMPv3 administrator. Only SNMP commands carrying this password are allowed to administer the ZyXEL Device.

Table 53 Remote Management: SNMP User Profile

LABEL	DESCRIPTION
Confirm Password	Re-enter the **Password**.
Access Type	For the administrator, this is always **Set**. SNMP Set commands allow the administrator to make configuration changes.
Authentication Protocol	Select an authentication algorithm. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy Protocol	Specify the encryption method for SNMP communication with this user. You can choose one of the following: • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. • **None** - no encryption is used.
Enable SNMPv3User	Select this box to activate the SNMPv3 user account. The SNMPv3 user can issue GET commands to the ZyXEL Device.
User Name	Enter a username for the SNMPv3 user. Only SNMP commands carrying this username are allowed to get details about the ZyXEL Device.
Password	Enter a password for the SNMPv3 administrator. Only SNMP commands carrying this password are allowed to get details about the ZyXEL Device.
Confirm Password	Re-enter the **Password**.
Access Type	For the administrator, this is always **Get**. SNMP Get commands allow the user to make see configuration details about the ZyXEL Device.
Authentication Protocol	Select an authentication algorithm. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy Protocol	Specify the encryption method for SNMP communication with this user. You can choose one of the following: • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. • **None** - no encryption is used.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

14

Internal RADIUS Server

The ZyXEL Device can use its internal RADIUS server to authenticate wireless clients. It can also serve as a RADIUS server to authenticate other APs and their wireless clients. For more background information on RADIUS, see Section 8.4 on page 119.

14.1 Internal RADIUS Overview

The ZyXEL Device has a built-in RADIUS server that can authenticate wireless clients or other trusted APs.

The ZyXEL Device can function as an AP and as a RADIUS server at the same time.

PEAP (Protected EAP) and MD5 authentication is implemented on the internal RADIUS server using simple username and password methods over a secure TLS connection. See the appendices for more information on the types of EAP authentication and the internal RADIUS authentication method used in your ZyXEL Device.

- Use the **AUTH. SERVER** > **Setting** screen to turn the ZyAIR's internal RADIUS server off or on and to view information about the ZyXEL Device's certificates.
- Use the **AUTH. SERVER** > **Trusted AP** screen to specify APs as trusted. Trusted APs can use the ZyAIR's internal RADIUS server to authenticate wireless clients.
- Use the **AUTH. SERVER** > **Trusted Users** screen to configure a list of wireless client user names and passwords for the ZyAIR to authenticate.

14.2 Internal RADIUS Server Setting

The **AUTH. SERVER** > **Setting** screen displays information about certificates. The certificates are used by wireless clients to authenticate the RADIUS server. Information matching the certificate is held on the wireless client's utility. A password and user name on the utility must match the **Trusted Users** list so that the RADIUS server can be authenticated.

The internal RADIUS server does not support domain accounts (DOMAIN/ user). When you configure your Windows XP SP2 Wireless Zero Configuration PEAP/MS-CHAPv2 settings, deselect the Use Windows logon name and password check box. When authentication begins, a pop-up dialog box requests you to type a Name, Password and Domain of the RADIUS server. Specify a name and password only, do not specify a domain.

Click **AUTH. SERVER > Setting**. The screen appears as shown.

Figure 100 Internal RADIUS Server Setting Screen

The following table describes the labels in this screen.

Table 54 Internal RADIUS Server Setting Screen Setting

LABEL	DESCRIPTION
Active	Select the **Active** check box to have the ZyXEL Device use its internal RADIUS server to authenticate wireless clients or other APs.
Index	This field displays the certificate index number. The certificates are listed in alphabetical order. Use the **CERTIFICATES** screens to manage certificates. The internal RADIUS server uses one of the certificates listed in this screen to authenticate each wireless client. The exact certificate used depends on the certificate information configured on the wireless client.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. **auto_generated_self_signed_cert** is the factory default certificate common to all ZyXEL Devices that use certificates. Note: It is recommended that you replace the factory default certificate with one that uses your ZyXEL Device's MAC address. Do this when you first log in to the ZyXEL Device or in the **CERTIFICATES > My Certificates** screen.

Table 54 Internal RADIUS Server Setting Screen Setting (continued)

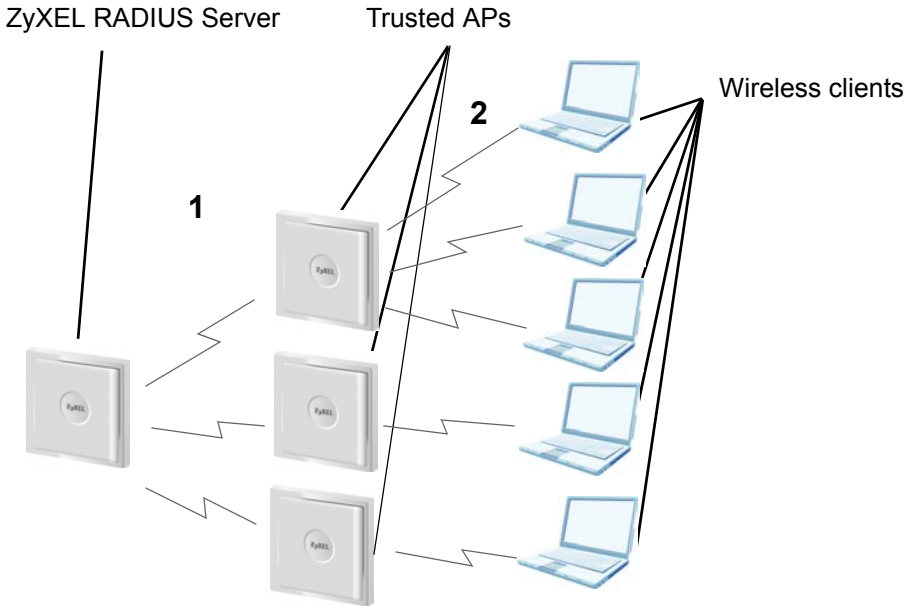
LABEL	DESCRIPTION
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Apply	Click **Apply** to have the ZyXEL Device use certificates to authenticate wireless clients.
Reset	Click **Reset** to start configuring this screen afresh.

14.3 Trusted AP Overview

A trusted AP is an AP that uses the ZyXEL Device's internal RADIUS server to authenticate its wireless clients. Each wireless client must have a user name and password configured in the **AUTH. SERVER** > **Trusted Users** screen.

The following figure shows how this is done in two phases.

Figure 101 Trusted AP Overview



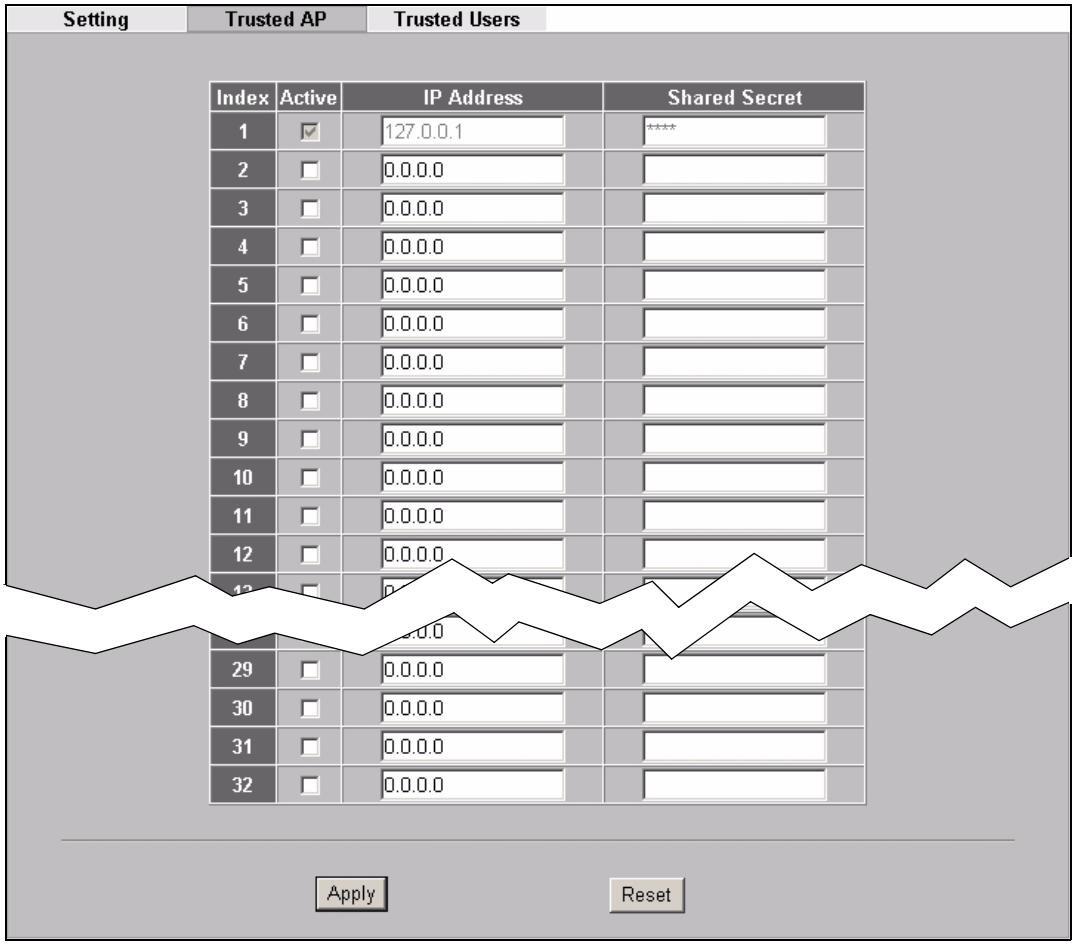
1 Configure an IP address and shared secret in the **Trusted AP** database to authenticate an AP as a trusted AP.

2 Configure wireless client user names and passwords in the **Trusted Users** database to use a trusted AP as a relay between the ZyXEL Device's internal RADIUS server and the wireless clients. The wireless clients can then be authenticated by the ZyXEL Device's internal RADIUS server.

14.4 Configuring Trusted AP

To specify trusted APs, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted AP** tab. The screen appears as shown.

Figure 102 Trusted AP Screen



The following table describes the labels in this screen.

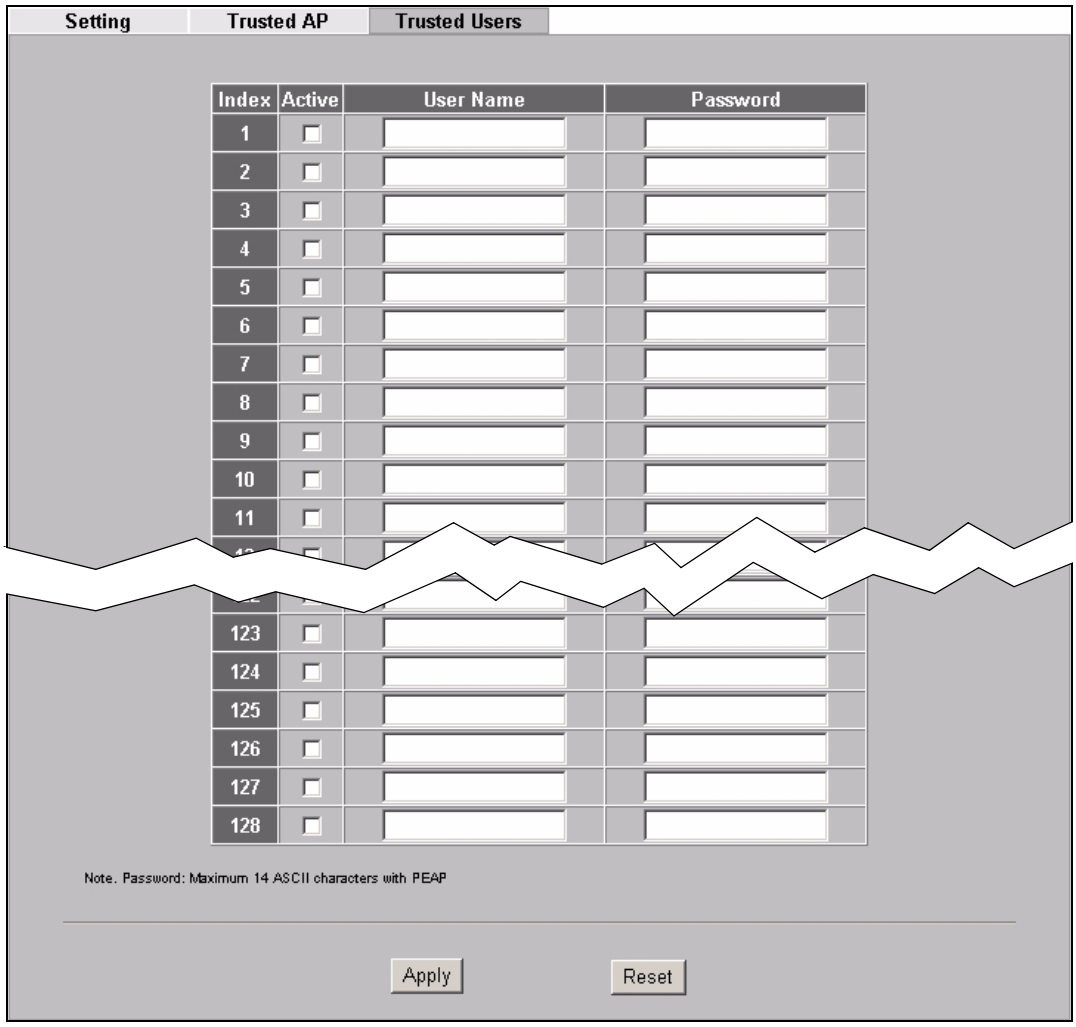
Table 55 Trusted AP

LABEL	DESCRIPTION
Index	This field displays the trusted AP index number.
Active	Select this check box to have the ZyXEL Device use the **IP Address** and **Shared Secret** to authenticate a trusted AP.
IP Address	Type the IP address of the trusted AP in dotted decimal notation.
Shared Secret	Enter a password (up to 31 alphanumeric characters, no spaces) as the key for encrypting communications between the AP and the ZyXEL Device. The key is not sent over the network. This key must be the same on the AP and the ZyXEL Device. Both the ZyXEL Device's IP address and this shared secret must also be configured in the "external RADIUS" server fields of the trusted AP. Note: The first trusted AP fields are for the ZyXEL Device itself.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

14.5 Configuring Trusted Users

A trusted user entry consists of a wireless client user name and password. To configure trusted user entries, click **AUTH SERVER** > **Trusted Users**. The screen appears as shown.

Figure 103 Trusted Users Screen



The following table describes the labels in this screen.

Table 56 Trusted Users

LABEL	DESCRIPTION
Index	This field displays the trusted user index number.
Active	Select this check box to have the ZyAIR authenticate wireless clients with the same user name and password activated on their wireless utilities.
User Name	Enter the user name for this user account. This name can be up to 31 alphanumeric characters long, including spaces. The wireless client's utility must use this name as its login name.

Table 56 Trusted Users

LABEL	DESCRIPTION
Password	Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. The password on the wireless client's utility must be the same as this password. Note: If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

15

Certificates

This chapter gives background information about public-key certificates and explains how to use them.

15.1 Certificates Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

15.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

15.2 Self-signed Certificates

You can have the ZyXEL Device act as a certification authority and sign its own certificates.

15.3 Verifying a Certificate

Before you import a trusted CA certificate into the ZyXEL Device, you should verify that you have the actual certificate. This is especially important since the ZyXEL Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

15.3.1 Checking the Fingerprint of a Certificate on Your Computer

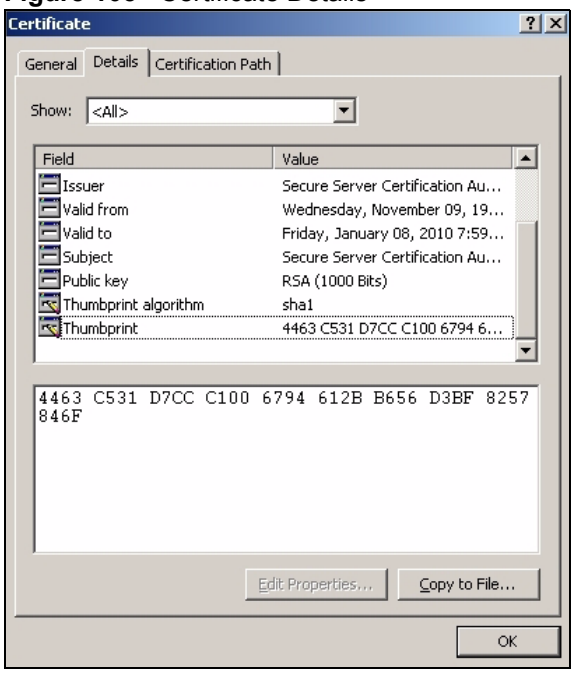
A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1. Browse to where you have the certificate saved on your computer.
2. Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 104 Certificates on Your Computer

3. Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 105 Certificate Details



4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary according to your situation. Possible examples would be over the telephone or through an HTTPS connection.

15.4 Configuration Summary

This section summarizes how to manage certificates.

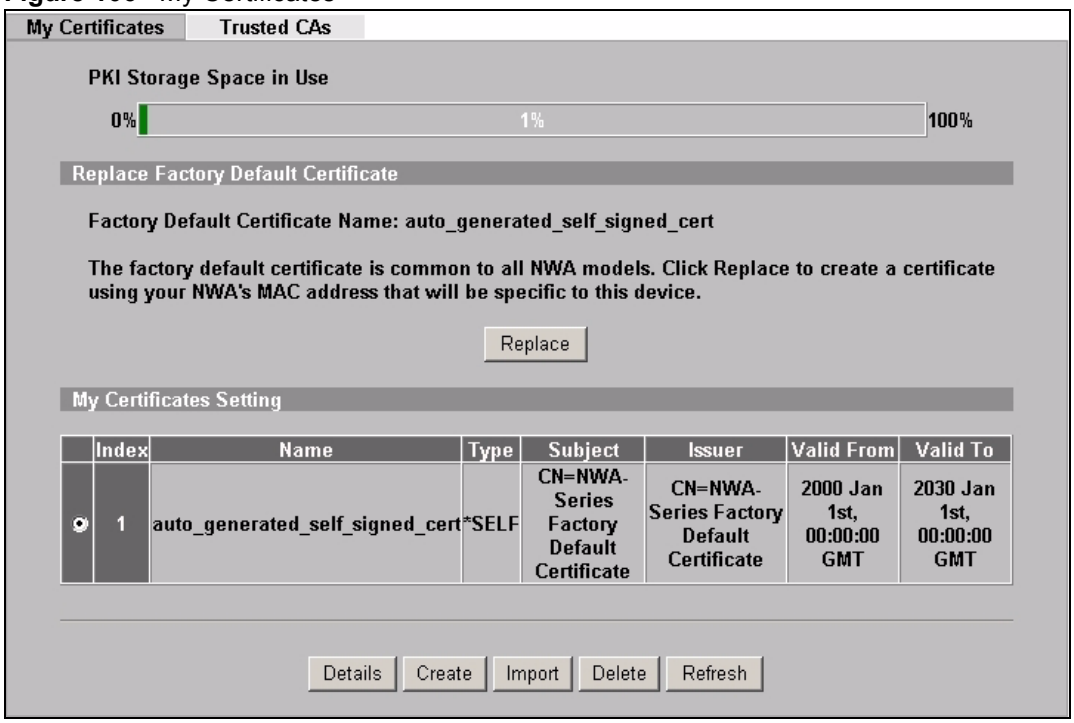
Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyXEL Devices' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the ZyXEL Device.

15.5 My Certificates

Click **CERTIFICATES** > **My Certificates** to open the ZyXEL Device's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

Figure 106 My Certificates



The following table describes the labels in this screen.

Table 57 My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyXEL Device has the factory default certificate. The factory default certificate is common to all ZyXEL Devices that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyXEL Device's MAC address.
Index	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

Table 57 My Certificates (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Details	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate. 2. Click the details icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. Note that subsequent certificates move up by one when you take this action
Create	Click **Create** to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.
Import	Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.
Delete	Click **Delete** to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Refresh	Click **Refresh** to display the current validity status of the certificates.

15.6 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

15.7 Importing a Certificate

Click **CERTIFICATES** > **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyXEL Device.

You can import only a certificate that matches a corresponding certification request that was generated by the ZyXEL Device.

The certificate you import replaces the corresponding request in the My Certificates screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 107 My Certificate Import

The following table describes the labels in this screen.

Table 58 My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

15.8 Creating a Certificate

Click **CERTIFICATES** > **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the ZyXEL Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request, see the following figure.

Figure 108 My Certificate Create

The following table describes the labels in this screen.

Table 59 My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the ZyXEL Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the ZyXEL Device generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (Section 15.9 on page 185) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.

Table 59 My Certificate Create (continued)

LABEL	DESCRIPTION
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SECP enrollment protocol.
Key	Type the key that the certification authority gave you.
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyXEL Device is generating the self-signed certificate or certification request.

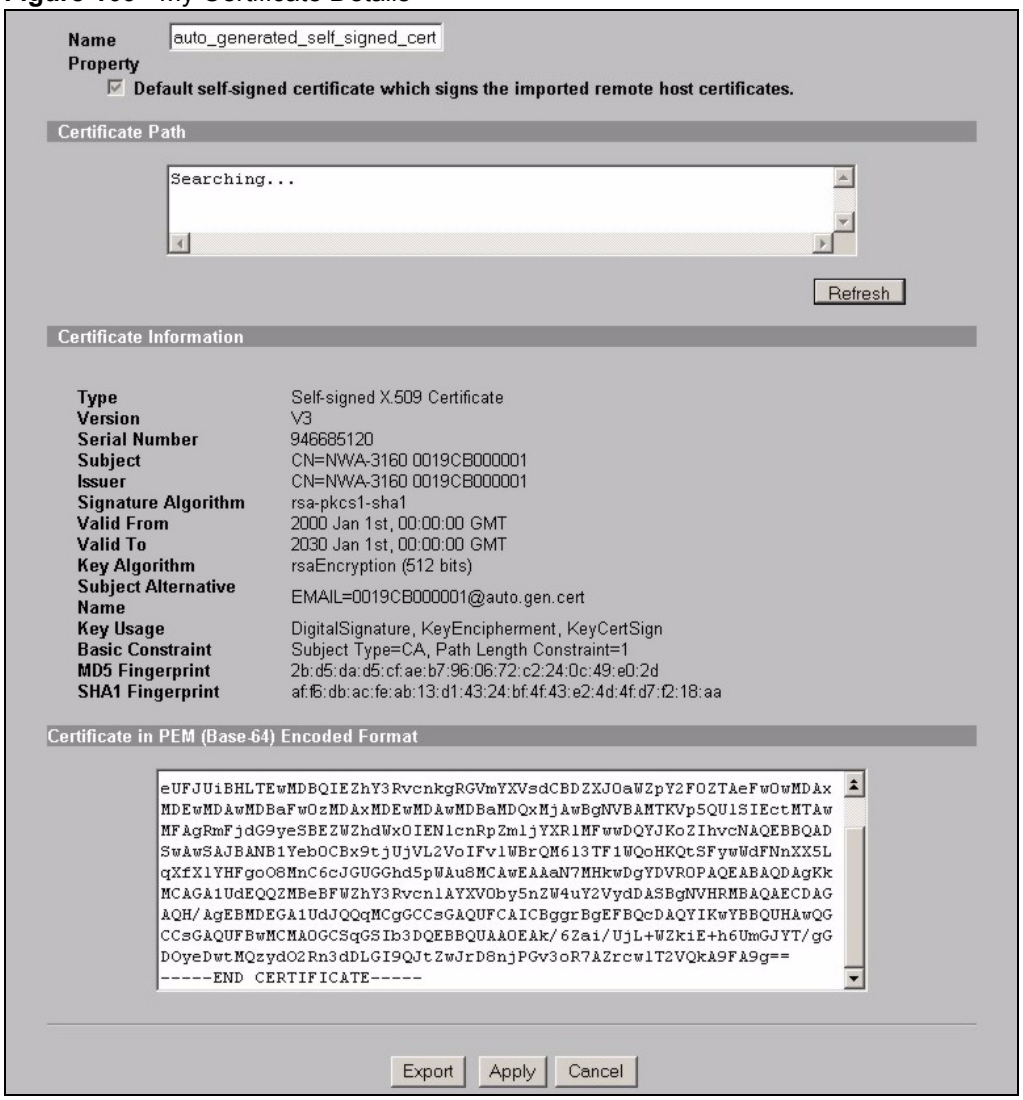
After the ZyXEL Device successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyXEL Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyXEL Device to enroll a certificate online.

15.9 My Certificate Details

Click **CERTIFICATES** > **My Certificates** to open the **My Certificates** screen (Figure 106 on page 180). Click the details button to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyXEL Device uses to sign the trusted remote host certificates that you import to the ZyXEL Device.

Figure 109 My Certificate Details



The following table describes the labels in this screen.

Table 60 My Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyXEL Device use this certificate to sign the trusted remote host certificates that you import to the ZyXEL Device. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.

Table 60 My Certificate Details (continued)

LABEL	DESCRIPTION
Certificate Path	Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyXEL Device does not trust the certificate and displays “Not trusted” in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate’s owner signed the certificate (not a certification authority). “X.509” means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate’s identification number given by the certification authority or generated by the ZyXEL Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate’s issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate’s key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner‘s IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path.
MD5 Fingerprint	This is the certificate’s message digest that the ZyXEL Device calculated using the MD5 algorithm.

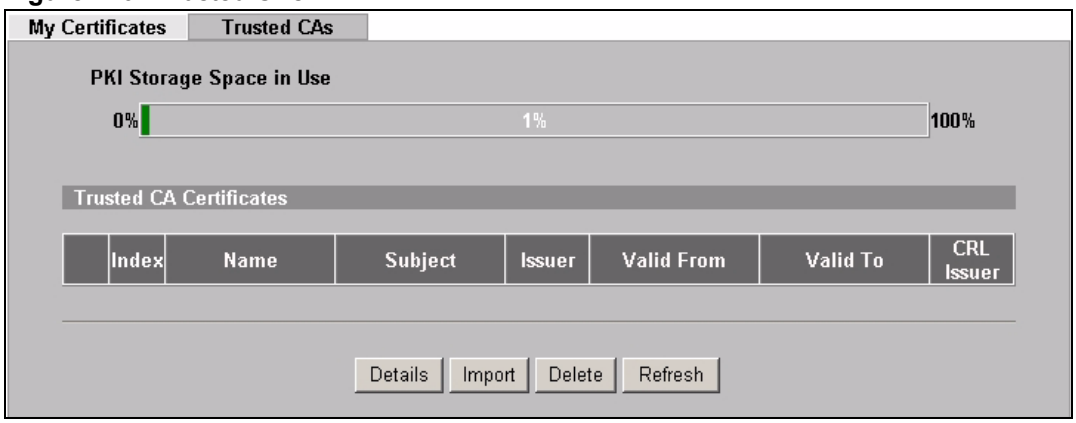
Table 60 My Certificate Details (continued)

LABEL	DESCRIPTION
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

15.10 Trusted CAs

Click **CERTIFICATES > Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. See the following figure.

Figure 110 Trusted CAs



The following table describes the labels in this screen.

Table 61 Trusted CAs

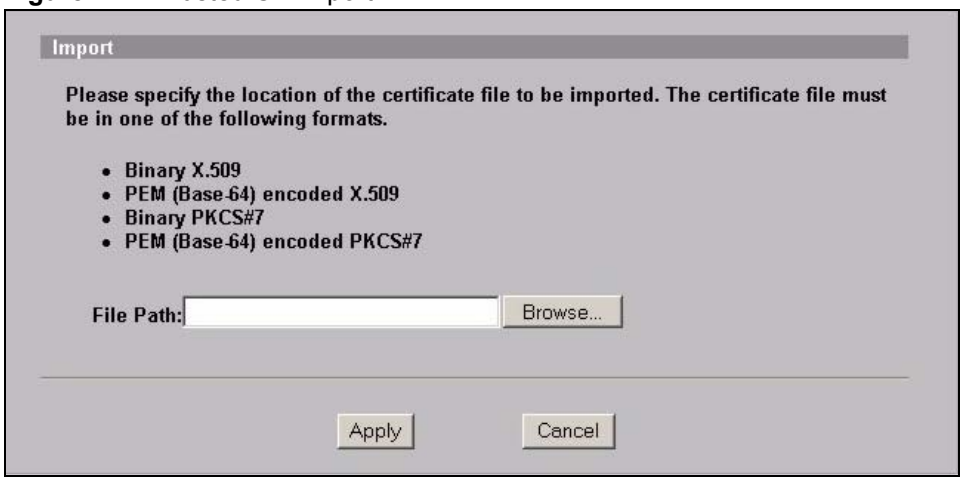
LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Index	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Details	Click **Details** to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Delete	Click **Delete** to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Refresh	Click this button to display the current validity status of the certificates.

15.11 Importing a Trusted CA's Certificate

Click **CERTIFICATES** >**Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device, see the following figure.

You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 111 Trusted CA Import



The following table describes the labels in this screen.

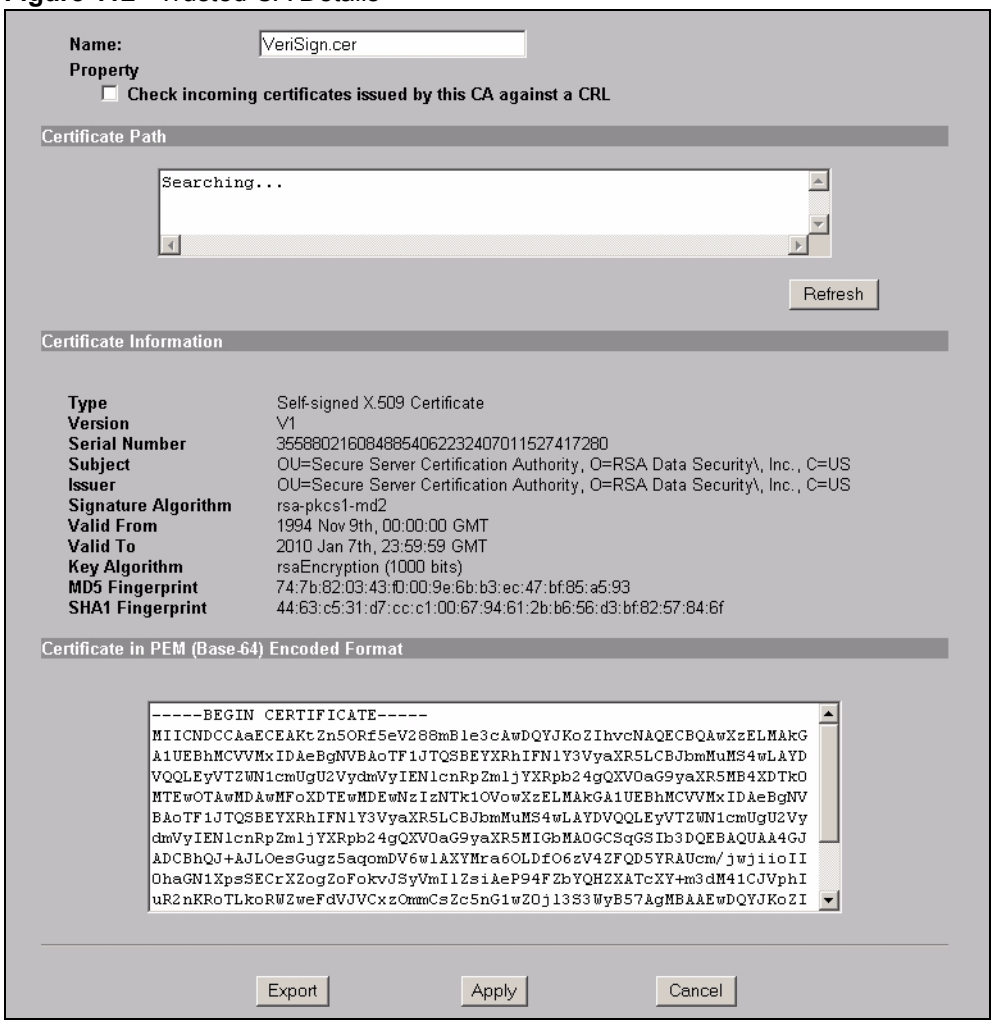
Table 62 Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

15.12 Trusted CA Certificate Details

Click **CERTIFICATES > Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 112 Trusted CA Details



The following table describes the labels in this screen.

Table 63 Trusted CA Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certificate Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.

Table 63 Trusted CA Details (continued)

LABEL	DESCRIPTION
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See Section 15.3 on page 178 for how to verify a remote host's certificate before you import it into the ZyXEL Device.

Table 63 Trusted CA Details (continued)

LABEL	DESCRIPTION
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See Section 15.3 on page 178 for how to verify a remote host's certificate before you import it into the ZyXEL Device.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

16

Log Screens

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs.

16.1 Configuring View Log

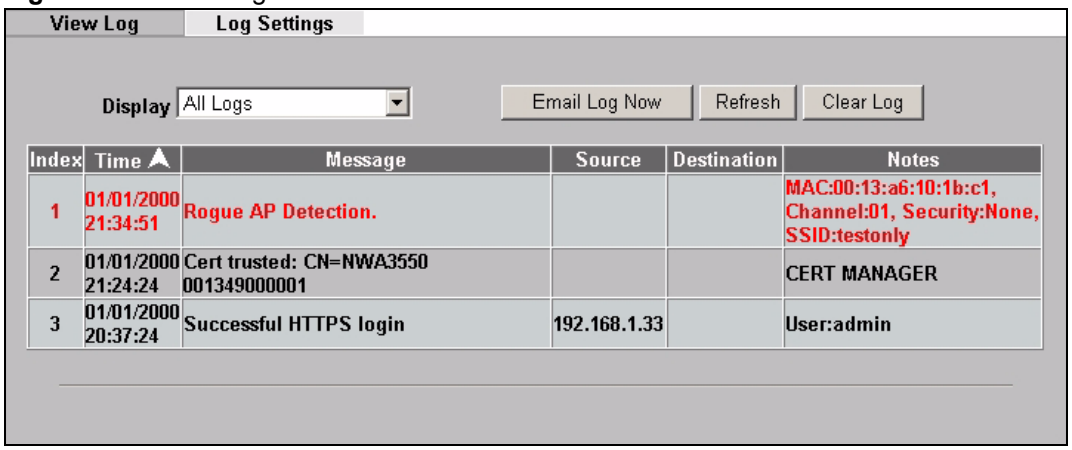
The web configurator allows you to look at all of the ZyXEL Device's logs in one location.

Click **LOGS > View Log**. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Figure 114 on page 197). Options include logs about system maintenance, system errors and access control.

You can view logs and alert messages in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

Figure 113 View Log



The following table describes the labels in this screen.

Table 64 View Log

LABEL	DESCRIPTION
Display	Select a log category from the drop down list box to display logs within the selected category. To view all logs, select **All Logs**. The number of categories shown in the drop down list box depends on the selection in the **Log Settings** page.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.

Table 64 View Log

LABEL	DESCRIPTION
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.

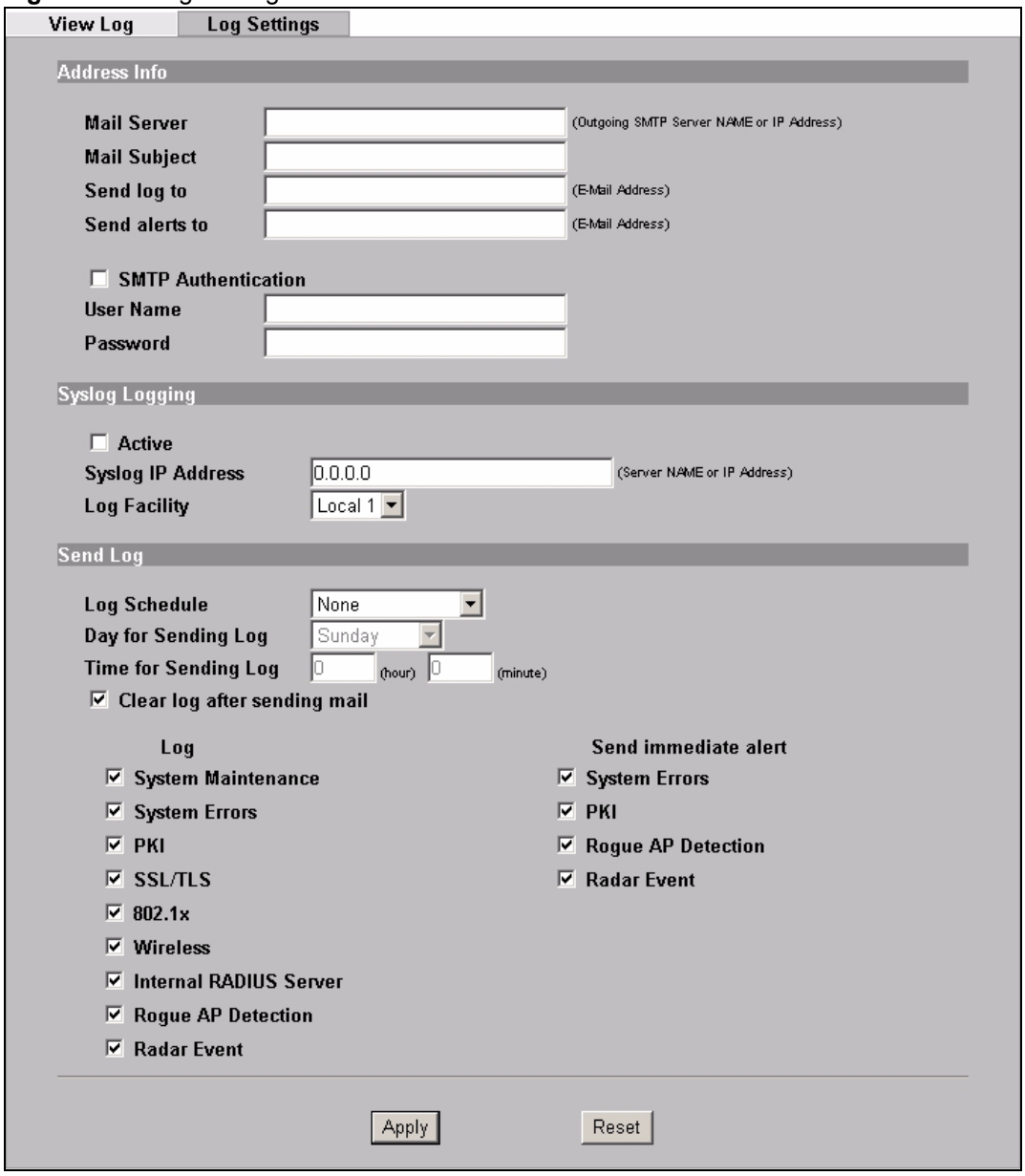
16.2 Configuring Log Settings

To change your ZyXEL Device's log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

Use the **Log Settings** screen to configure to where and when the ZyXEL Device is to send the logs and which logs and/or immediate alerts it is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

Figure 114 Log Settings



The following table describes the labels in this screen.

Table 65 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends.
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts to	Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.

Table 65 Log Settings

LABEL	DESCRIPTION
SMTP Authentication	If you use SMTP authentication, the mail receiver should be the owner of the SMTP account.
User Name	If your e-mail account requires SMTP authentication, enter the username here.
Password	Enter the password associated with the above username.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select the categories of alerts for which you want the ZyXEL Device to immediately send e-mail alerts.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to reconfigure all the fields in this screen.

16.3 Example Log Messages

This section provides descriptions of some example log messages.

Table 66 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.

Table 66 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
SMT Login Successfully	Someone has logged on to the router's SMT interface.
SMT Login Fail	Someone has failed to log on to the router's SMT interface.
WEB Login Successfully	Someone has logged on to the router's web configurator interface.
WEB Login Fail	Someone has failed to log on to the router's web configurator interface.
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
FTP Login Successfully	Someone has logged on to the router via FTP.
FTP Login Fail	Someone has failed to log on to the router via FTP.

Table 67 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem

Table 67 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 68 Sys log

LOG MESSAGE	DESCRIPTION
Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>"	This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts.

16.4 Log Commands

Go to the command interpreter interface (see Chapter 25 on page 257 for how to access and use the commands).

16.4.1 Configuring What You Want the ZyXEL Device to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

Table 69 Log Categories and Available Settings Example

LOG CATEGORIES	AVAILABLE PARAMETERS
error	0, 1, 2, 3
mten	0, 1
Use `0` to not record logs for that category, `1` to record only logs for that category, `2` to record only alerts for that category, and `3` to record both logs and alerts for that category.	

Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

16.4.2 Displaying Logs

Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual ZyXEL Device log category.

Use the `sys logs clear` command to erase all of the ZyXEL Device's logs.

16.5 Log Command Example

This example shows how to set the ZyXEL Device to record the error logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access

#.    time                  source              destination           notes    message
0   | 11/11/2002 15:10:12 | 172.22.3.80:137   |  172.22.255.255:137   |  ACCESS   BLOCK
```

17 VLAN

This chapter discusses how to configure VLAN on the ZyXEL Device.

17.1 VLAN

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network can belong to one or more groups. Only stations within the same group can talk to each other.

17.1.1 Management VLAN ID

The Management VLAN ID identifies the “management VLAN”. A device must be a member of this “management VLAN” in order to access and manage the ZyXEL Device. If a device is not a member of this VLAN, then that device cannot manage the ZyXEL Device.

If no devices are in the management VLAN, then you will be able to access the ZyXEL Device only through the console port (not through the network).

17.1.2 VLAN Tagging

The ZyXEL Device supports IEEE 802.1q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The ZyXEL Device can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.

You must connect the ZyXEL Device to a VLAN-aware device that is a member of the management VLAN in order to perform management. See the Configuring Management VLAN Example BEFORE you configure the VLAN screens.

17.2 Configuring VLAN

The ZyXEL Device allows you to configure VLAN based on SSID profile (wireless VLAN), and / or based on your RADIUS server (RADIUS VLAN).

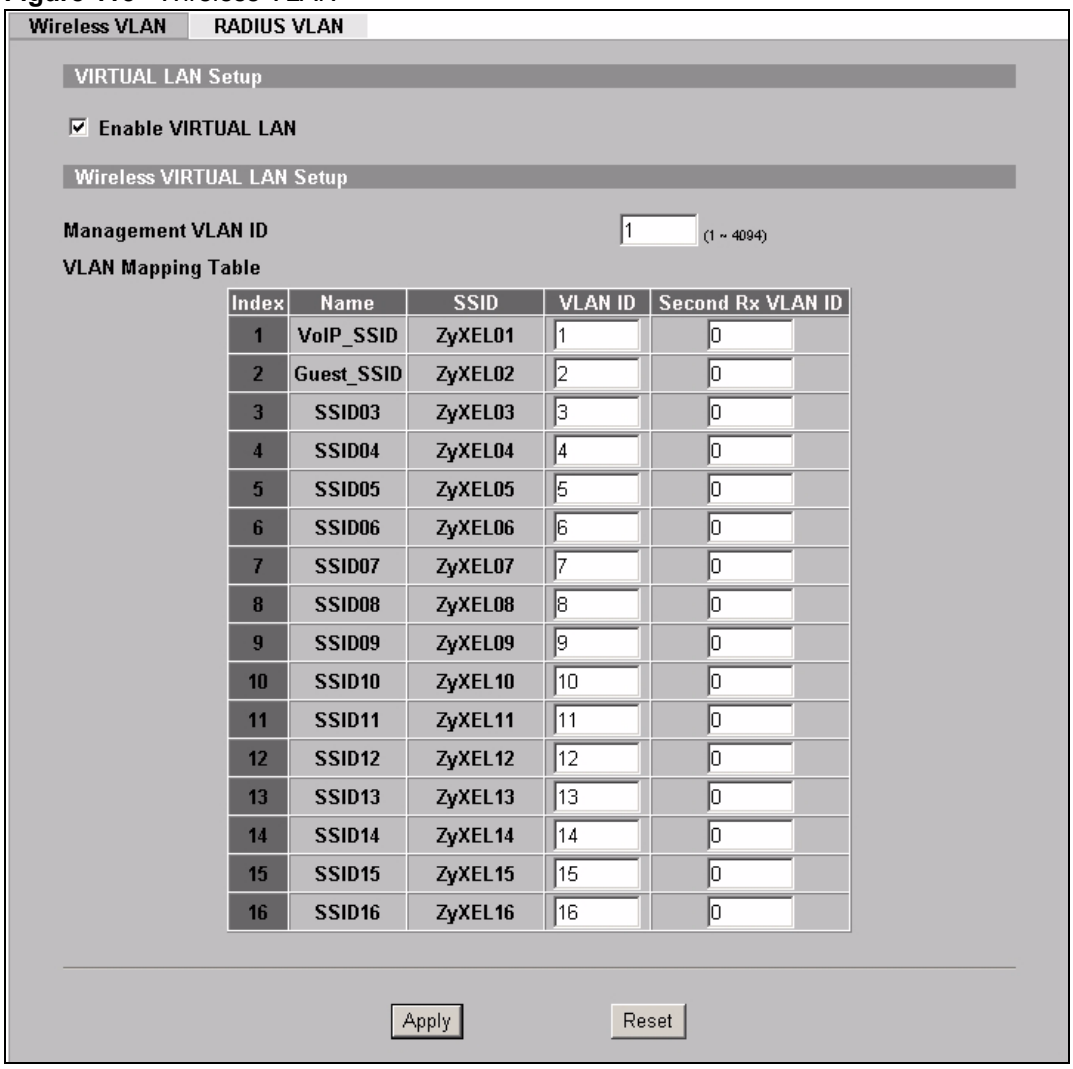
- When you use wireless VLAN, the ZyXEL Device tags all packets from an SSID with the VLAN ID you set in the **Wireless VLAN** screen.
- When you use RADIUS VLAN, your RADIUS server assigns VLAN IDs to a user or user group's traffic based on the configuration in the **RADIUS VLAN** screen.
- When you use wireless VLAN and RADIUS VLAN together, the ZyXEL Device first tries to assign VLAN IDs based on RADIUS VLAN configuration. If a client's user name does not match an entry in the **RADIUS VLAN** screen, the ZyXEL Device assigns a VLAN ID based on the settings in the **Wireless VLAN** screen. See Section 17.2.4 on page 210 for more information.

To use RADIUS VLAN, you must first select **Enable VIRTUAL LAN** and configure the **Management VLAN ID** in the **VLAN > Wireless VLAN** screen.

17.2.1 Wireless VLAN

Click **VLAN** > **Wireless VLAN**. The following screen appears.

Figure 115 Wireless VLAN



The following table describes the labels in this screen

Table 70 Wireless VLAN

FIELD	DESCRIPTION
Enable VIRTUAL LAN	Select this box to enable VLAN tagging.
Management VLAN ID	Enter a number from 1 to 4094 to define this VLAN group. At least one device in your network must belong to this VLAN group in order to manage the ZyXEL Device. Note: Mail and FTP servers must have the same management VLAN ID to communicate with the ZyXEL Device. See Section 17.2.3 on page 207 for more information.
VLAN Mapping Table	Use this table to have the ZyXEL Device assign VLAN tags to packets from wireless clients based on the SSID they use to connect to the ZyXEL Device.
Index	This is the index number of the SSID profile.

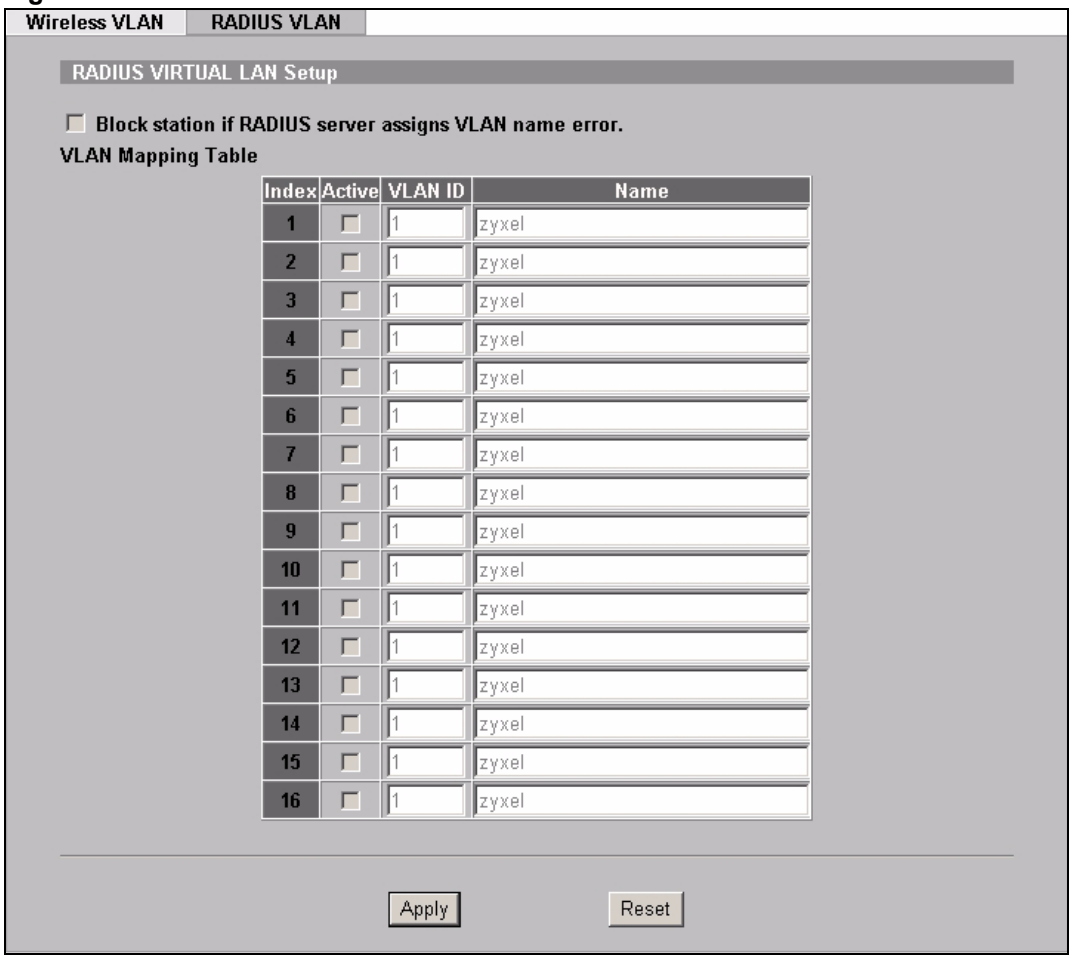
Table 70 Wireless VLAN

FIELD	DESCRIPTION
Name	This is the name of the SSID profile.
SSID	This is the SSID the profile uses.
VLAN ID	Enter a VLAN ID number from 1 to 4094. Packets coming from the WLAN using this SSID profile are tagged with the VLAN ID number by the ZyXEL Device. Different SSID profiles can use the same or different VLAN IDs. This allows you to split wireless stations into groups using similar VLAN IDs.
Second Rx VLAN ID	Enter a number from 1 to 4094, but different from the entry's **VLAN ID**. Traffic received from the LAN that is tagged with this VLAN ID is sent to all SSIDs with this VLAN ID configured in the **VLAN ID** or **Second Rx VLAN ID** fields. See Section 17.2.5 on page 218 for more information.
Apply	Click this to save your changes to the ZyXEL Device.
Reset	Click this to return this screen to its last-saved settings.

17.2.2 RADIUS VLAN

Click **VLAN** > **RADIUS VLAN**. The following screen appears.

Figure 116 RADIUS VLAN



The following table describes the labels in this screen.

Table 71 RADIUS VLAN

LABEL	DESCRIPTION
Block station if RADIUS server assigns VLAN name error!	Select this to have the ZyXEL Device forbid access to wireless clients when the VLAN attributes sent from the RADIUS server do not match a configured **Name** field. When you select this check box, only users with names configured in this screen can access the network through the ZyXEL Device.
VLAN Mapping Table	Use this table to map names to VLAN IDs so that the RADIUS server can assign each user or user group a mapped VLAN ID. See your RADIUS server documentation for more information on configuring VLAN ID attributes. See Section 17.2.4 on page 210 for more information.
Index	This is the index number of the VLAN mapping profile.
Active	Select a check box to enable the VLAN mapping profile.
VLAN ID	Type a VLAN ID. Incoming traffic from the WLAN is authorized and assigned a VLAN ID before it is sent to the LAN.
Name	Type a name to have the ZyXEL Device check for specific VLAN attributes on incoming messages from the RADIUS server. Access-accept packets sent by the RADIUS server contain VLAN related attributes. The configured **Name** fields are checked against these attributes. If a configured **Name** field matches these attributes, the corresponding VLAN ID is added to packets sent from this user to the LAN. If the VLAN-related attributes sent by the RADIUS server do not match a configured **Name** field, a wireless station is assigned the wireless VLAN ID associated with its SSID (unless the **Block station if RADIUS server assigns VLAN error!** check box is selected).
Apply	Click **Apply** to save your changes to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.

17.2.3 Configuring Management VLAN Example

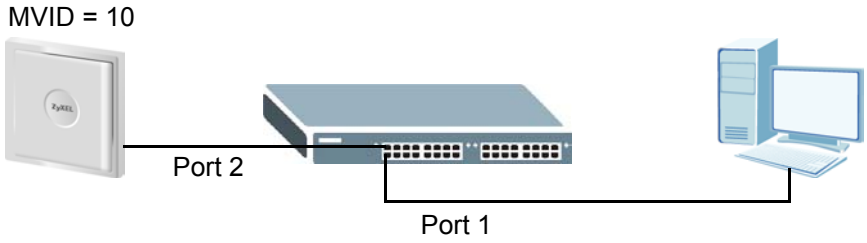
This section shows you how to create a VLAN on an Ethernet switch.

By default, the port on the ZyXEL Device is a member of the management VLAN (VLAN ID 1). The following procedure shows you how to configure a tagged VLAN.

Use the out-of-band management port or console port to configure the switch if you misconfigure the management VLAN and lock yourself out from performing in-band management.

On an Ethernet switch, create a VLAN that has the same management VLAN ID as the ZyXEL Device. The following figure has the ZyXEL Device connected to port 2 of the switch and your computer connected to port 1. The management VLAN ID is ten.

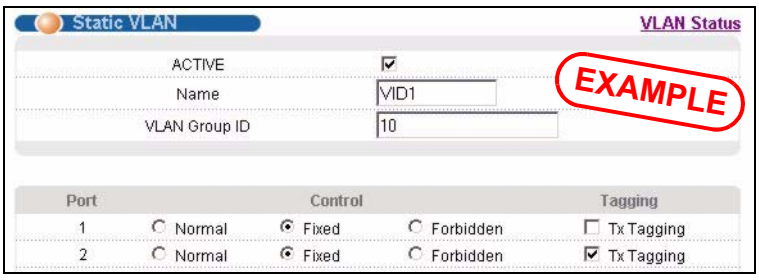
Figure 117 Management VLAN Configuration Example



Perform the following steps in the switch web configurator. This example uses the ZyXEL switch screenshots.

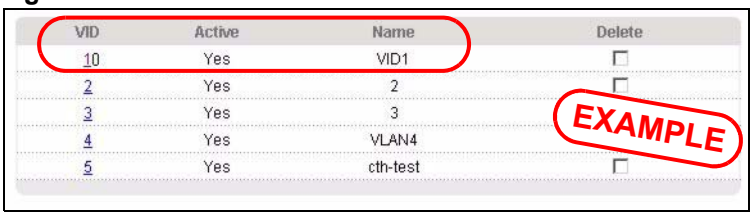
1. Click **VLAN** under **Advanced Application**.
2. Click **Static VLAN**.
3. Select the **ACTIVE** check box.
4. Type a **Name** for the VLAN ID.
5. Type a **VLAN Group ID**. This should be the same as the management VLAN ID on the ZyXEL Device.
6. Enable **Tx Tagging** on the port which you want to connect to the ZyXEL Device. Disable **Tx Tagging** on the port you are using to connect to your computer.
7. Under **Control**, select **Fixed** to set the ports (1 and 2 in this example) as a member of the VLAN.

Figure 118 VLAN-Aware Switch - Static VLAN



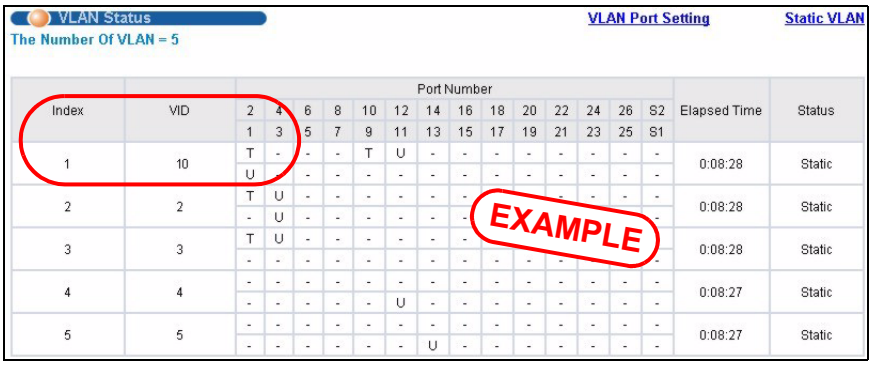
8. Click **Apply**. The following screen displays.

Figure 119 VLAN-Aware Switch



9. Click **VLAN Status** to display the following screen.

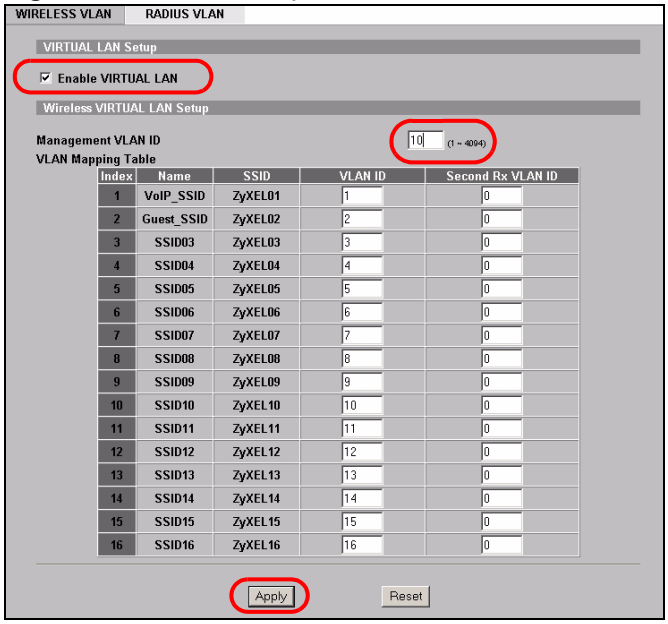
Figure 120 VLAN-Aware Switch - VLAN Status



Follow the instructions in the Quick Start Guide to set up your ZyXEL Device for configuration. The ZyXEL Device should be connected to the VLAN-aware switch. In the above example, the switch is using port 1 to connect to your computer and port 2 to connect to the ZyXEL Device: Figure 117 on page 208.

1. In the ZyXEL Device web configurator click **VLAN** to open the VLAN setup screen.
2. Select the **Enable VIRTUAL LAN** check box and type a **Management VLAN ID** (10 in this example) in the field provided.
3. Click **Apply**.

Figure 121 VLAN Setup



4. The ZyXEL Device attempts to connect with a VLAN-aware device. You can now access and mange the ZyXEL Device though the Ethernet switch.

If you do not connect the ZyXEL Device to a correctly configured VLAN-aware device, you will lock yourself out of the ZyXEL Device. If this happens, you must reset the ZyXEL Device to access it again.

17.2.4 Configuring Microsoft's IAS Server Example

Dynamic VLAN assignment can be used with the ZyXEL Device. Dynamic VLAN assignment allows network administrators to assign a specific VLAN (configured on the ZyXEL Device) to an individual's Windows User Account. When a wireless station is successfully authenticated to the network, it is automatically placed into it's respective VLAN.

ZyXEL uses the following standard RADIUS attributes returned from Microsoft's IAS (Internet Authentication Service) RADIUS service to place the wireless station into the correct VLAN:

Table 72 Standard RADIUS Attributes

ATTRIBUTE NAME	TYPE	VALUE
Tunnel-Type	064	13 (decimal) – VLAN
Tunnel-Medium-Type	065	6 (decimal) – 802
Tunnel-Private-Group-ID	081	<vlan-name> (string) – either the **Name** you enter in the ZyXEL Device's **VLAN > RADIUS VLAN** screen or the number. See Figure 133 on page 216.

The following occurs under Dynamic VLAN Assignment:

1. When you configure your wireless credentials, the ZyXEL Device sends the information to the IAS server using RADIUS protocol.
2. Authentication by the RADIUS server is successful.
3. The RADIUS server sends three attributes related to this feature.
4. The ZyXEL Device compares these attributes with the VLAN screen mapping table.
   - **4a** If the **Name**, for example "VLAN 20" is found, the mapped VLAN ID is used.
   - **4b** If the **Name** is not found in the mapping table, the string in the **Tunnel-Private-Group-ID** attribute is considered as a number ID format, for example 2493. The range of the number ID (Name:string) is between 1 and 4094.
   - **4c** If **a** or **b** are not matched, the ZyXEL Device uses the VLAN ID configured in the **Wireless VLAN** screen and the wireless station. The **VLAN ID** in the **Wireless VLAN** screen is independent and hence different to the **VLAN ID** in the **RADIUS VLAN** screen.

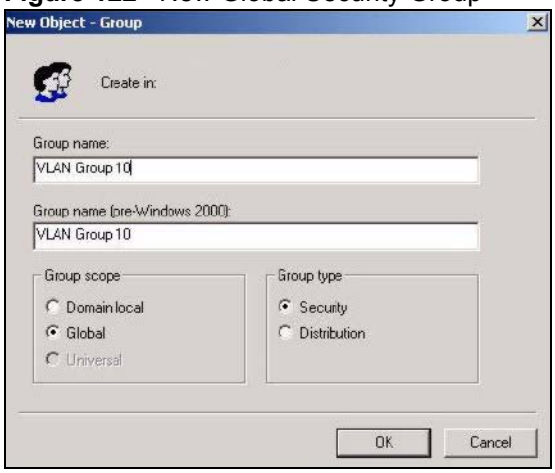
17.2.4.1 Configuring VLAN Groups

To configure a VLAN group you must first define the VLAN Groups on the Active Directory server and assign the user accounts to each VLAN Group.

1. Using the Active Directory Users and Computers administrative tool, create the VLAN Groups that will be used for each VLAN ID. One VLAN Group must be created for each VLAN defined on the ZyXEL Device. The VLAN Groups must be created as **Global/ Security** groups.

- Type a name for the **VLAN Group** that describes the VLAN Group's function.
- Select the **Global** Group scope parameter check box.
- Select the **Security** Group type parameter check box.
- Click **OK**.

Figure 122 New Global Security Group

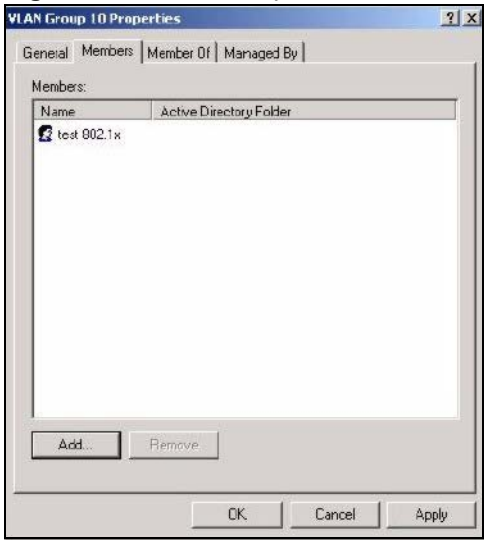


2 In **VLAN Group ID Properties**, click the **Members** tab.

- The IAS uses group memberships to determine which user accounts belong to which VLAN groups. Click the **Add** button and configure the VLAN group details.

3 Repeat the previous step to add each VLAN group required.

Figure 123 Add Group Members



17.2.4.2 Configuring Remote Access Policies

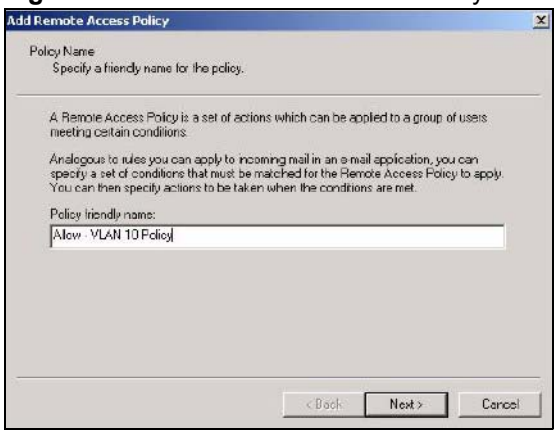
Once the VLAN Groups have been created, the IAS Remote Access Policy needs to be defined. This allows the IAS to compare the user account being authenticated against the group memberships of each VLAN Group.

1 Using the **Remote Access Policy** option on the Internet Authentication Service management interface, create a new VLAN Policy for each VLAN Group defined in the previous section. The order of the remote access policies is important. The most specific policies should be placed at the top of the policy list and the most general at the bottom. For example, if the Day-And-Time Restriction policy is still present, it should be moved to the bottom or deleted to allow the VLAN Group policies to take precedence.

- Right click **Remote Access Policy** and select **New Remote Access Policy**.

- Enter a **Policy friendly name** that describes the policy. Each Remote Access Policy will be matched to one VLAN Group. An example may be, **Allow - VLAN 10 Policy**.
- Click **Next**.

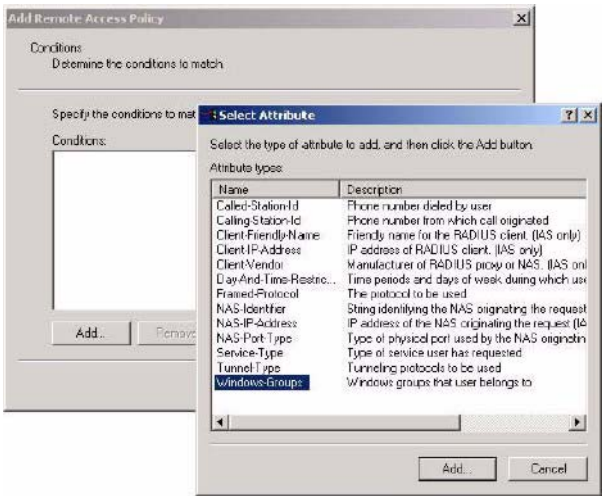
Figure 124 New Remote Access Policy for VLAN Group



2 The **Conditions** window displays. Select **Add** to add a condition for this policy to act on.

3 In the **Select Attribute** screen, click **Windows-Groups** and the **Add** button.

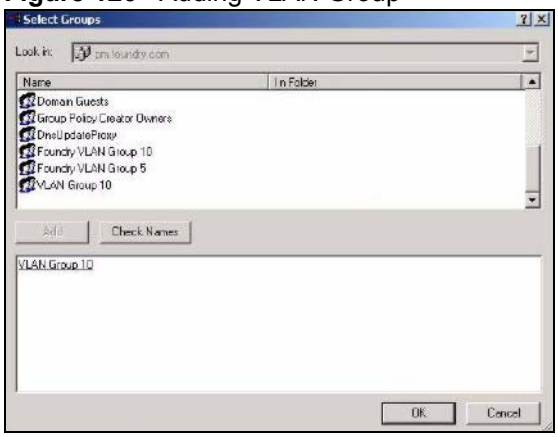
Figure 125 Specifying Windows-Group Condition



4 The **Select Groups** window displays. Select a remote access policy and click the **Add** button. The policy is added to the field below. Only one VLAN Group should be associated with each policy.

5 Click **OK** and **Next** in the next few screens to accept the group value.

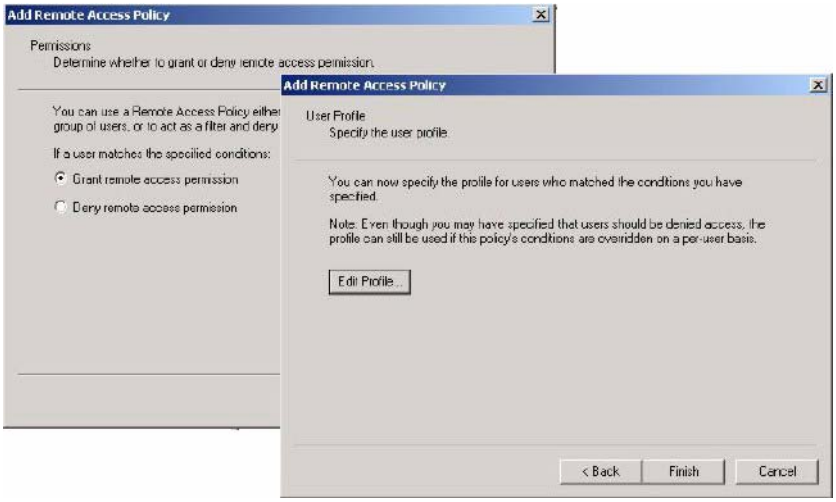
Figure 126 Adding VLAN Group



6 When the **Permissions** options screen displays, select **Grant remote access permission**.

- Click **Next** to grant access based on group membership.
- Click the **Edit Profile** button.

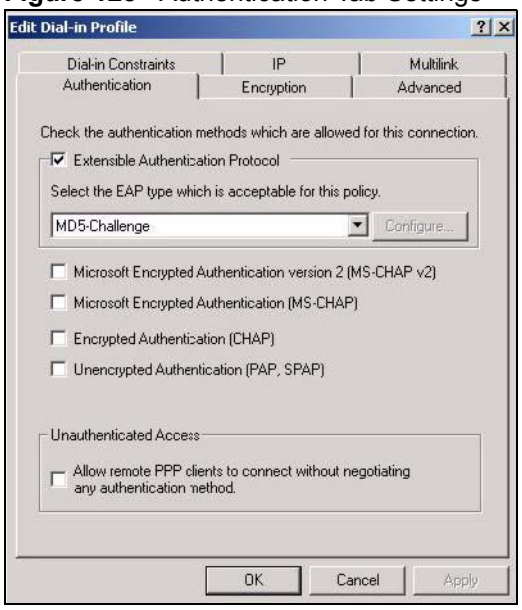
Figure 127 Granting Permissions and User Profile Screens



7 The **Edit Dial-in Profile** screen displays. Click the **Authentication** tab and select the **Extensible Authentication Protocol** check box.

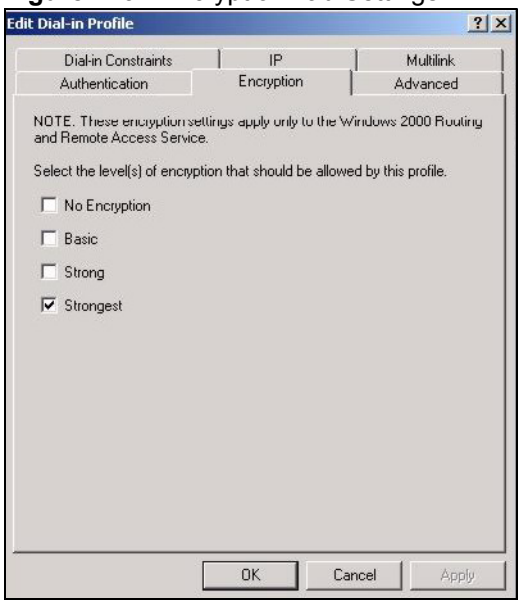
- Select an EAP type depending on your authentication needs from the drop-down list box.
- Clear the check boxes for all other authentication types listed below the drop-down list box.

Figure 128 Authentication Tab Settings



8 Click the **Encryption** tab. Select the **Strongest** encryption option. This step is not required for EAP-MD5, but is performed as a safeguard.

Figure 129 Encryption Tab Settings

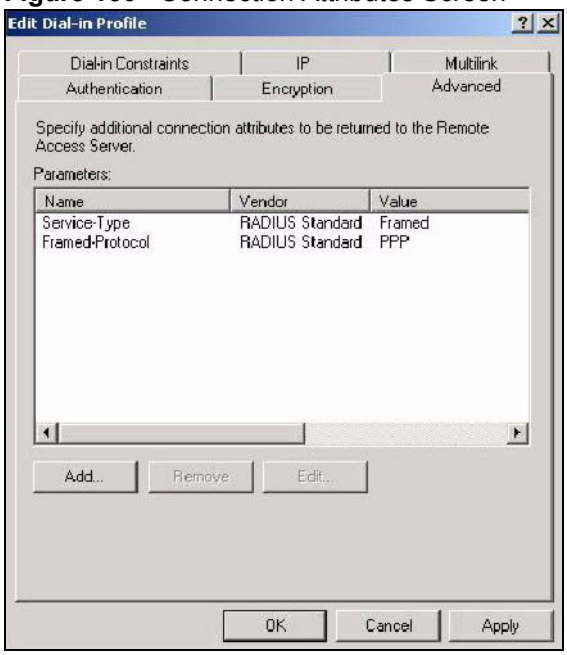


9 Click the **IP** tab and select the **Client may request an IP address** check box for DHCP support.

10 Click the **Advanced** tab. The current default parameters returned to the ZyXEL Device should be **Service-Type** and **Framed-Protocol**.

- Click the **Add** button to add an additional three RADIUS VLAN attributes required for 802.1X Dynamic VLAN Assignment.

Figure 130 Connection Attributes Screen

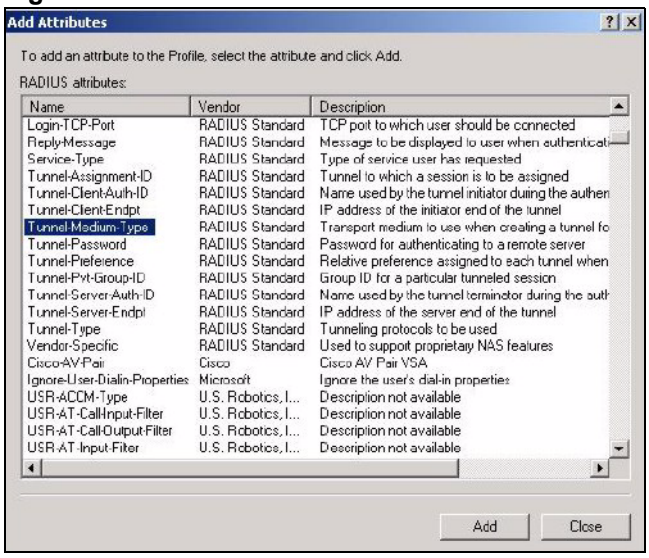


11 The RADIUS Attribute screen displays. From the list, three RADIUS attributes will be added:

- Tunnel-Medium-Type
- Tunnel-Pvt-Group-ID
- Tunnel-Type

- Click the **Add** button
- Select **Tunnel-Medium-Type**
- Click the **Add** button.

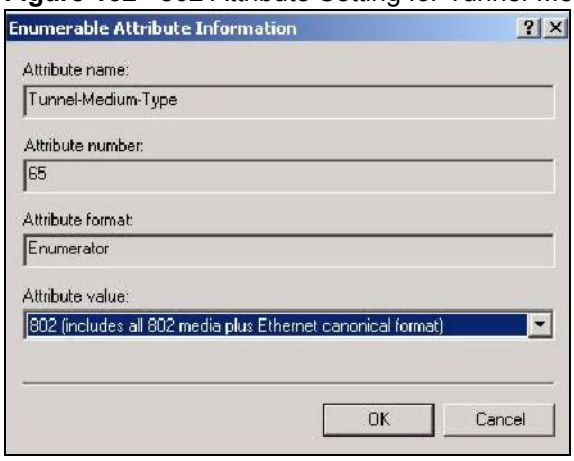
Figure 131 RADIUS Attribute Screen



12 The **Enumerable Attribute Information** screen displays. Select the **802** value from the **Attribute value** drop-down list box.

- Click **OK**.

Figure 132 802 Attribute Setting for Tunnel-Medium-Type



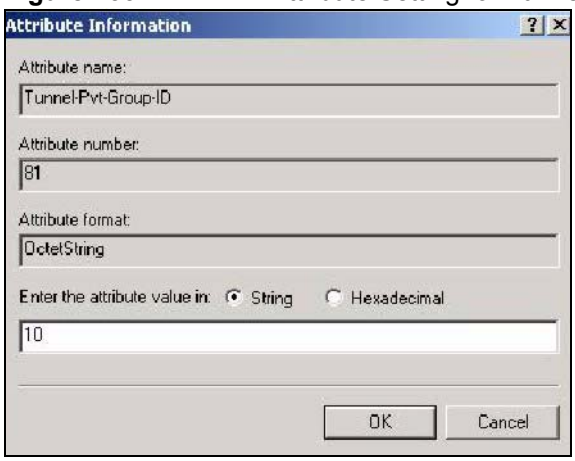
13 Return to the **RADIUS Attribute Screen** shown as Figure 131 on page 215.

- Select **Tunnel-Pvt-Group-ID.**
- Click **Add**.

14 The **Attribute Information** screen displays.

- In the **Enter the attribute value in:** field select **String** and type a number in the range 1 to 4094 or a **Name** for this policy. This **Name** should match a name in the VLAN mapping table on the ZyXEL Device. Wireless stations belonging to the VLAN Group specified in this policy will be given a VLAN **ID** specified in the ZyXEL Device VLAN table.
- Click **OK**.

Figure 133 VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID



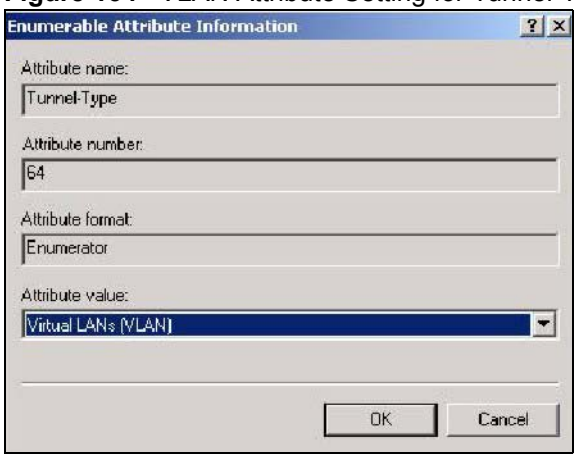
15 Return to the **RADIUS Attribute Screen** shown as Figure 131 on page 215.

- Select **Tunnel-Type**.
- Click **Add**.

16 The **Enumerable Attribute Information** screen displays.

- Select **Virtual LANs (VLAN)** from the attribute value drop-down list box.
- Click **OK**.

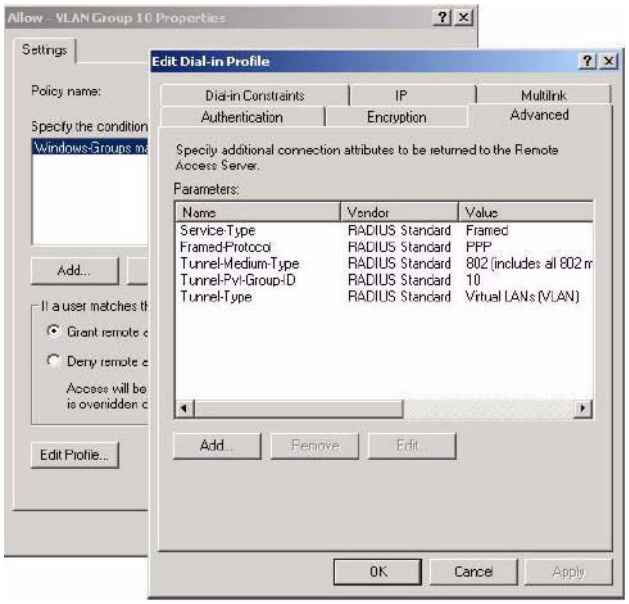
Figure 134 VLAN Attribute Setting for Tunnel-Type



17 Return to the **RADIUS Attribute Screen** shown as Figure 131 on page 215.

- Click the **Close** button.
- The completed **Advanced** tab configuration should resemble the following screen.

Figure 135 Completed Advanced Tab

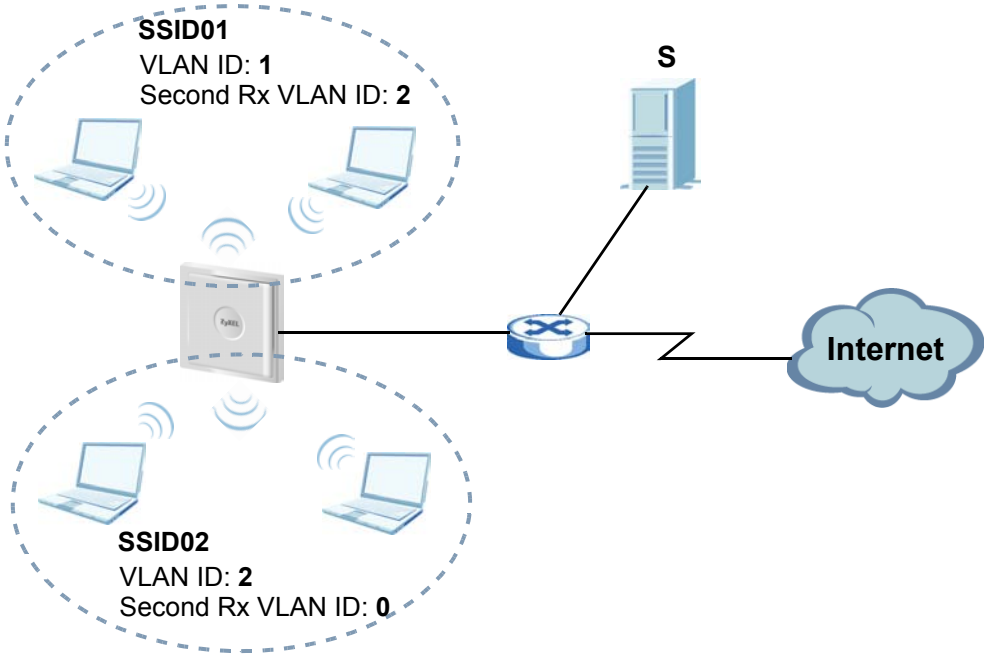


Repeat the Configuring Remote Access Policies procedure for each VLAN Group defined in the Active Directory. Remember to place the most general Remote Access Policies at the bottom of the list and the most specific at the top of the list.

17.2.5 Second Rx VLAN ID Example

In this example, the ZyXEL Device is configured to tag packets from **SSID01** with VLAN ID 1 and tag packets from **SSID02** with VLAN ID 2. **VLAN 1** and **VLAN 2** have access to a server, **S**, and the Internet, as shown in the following figure.

Figure 136 Second Rx VLAN ID Example



Packets sent from the server **S** back to the switch are tagged with a VLAN ID (incoming VLAN ID). These incoming VLAN packets are forwarded to the ZyXEL Device. The ZyXEL Device compares the VLAN ID in the packet header with each SSID's configured VLAN ID and second Rx VLAN ID settings.

In this example, **SSID01**'s second Rx VLAN ID is set to **2**. All incoming packets tagged with VLAN ID **2** are forwarded to **SSID02**, and also to **SSID01**. However, **SSID02** has no second Rx VLAN ID configured, and the ZyXEL Device forwards only packets tagged with VLAN ID **2** to it.

17.2.5.1 Second Rx VLAN Setup Example

The following steps show you how to setup a second Rx VLAN ID on the ZyXEL Device.

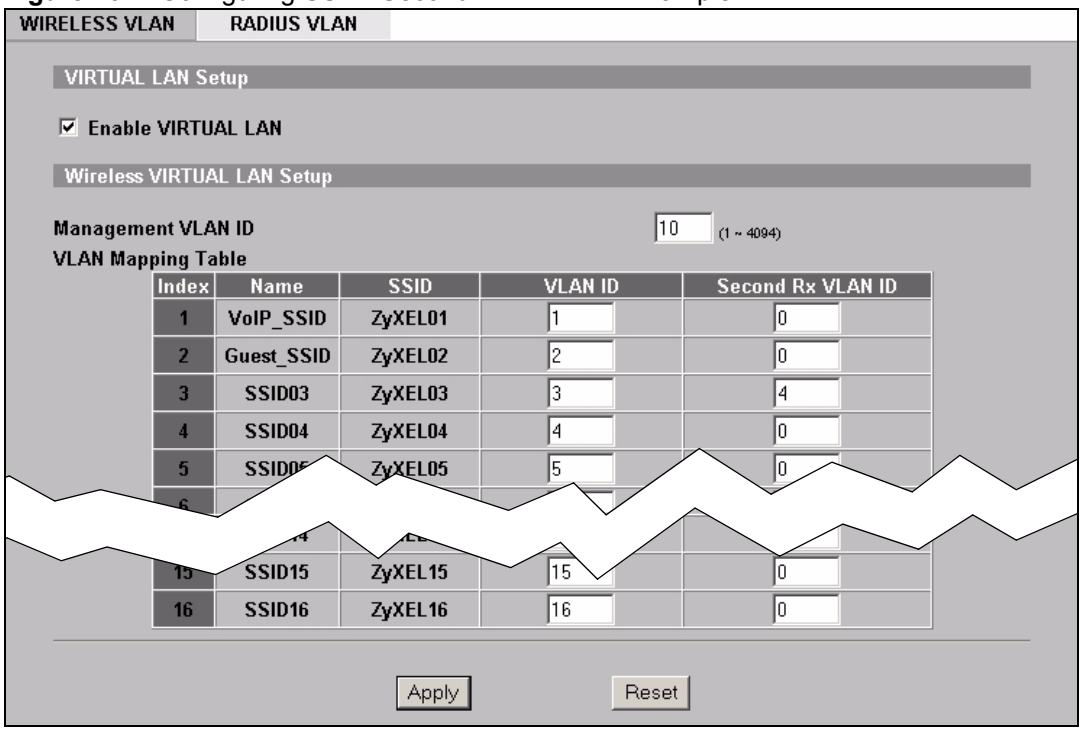
1. Log into the Web Configurator.
2. Click **VLAN > Wireless VLAN**.
3. If VLAN is not already enabled, click **Enable VIRTUAL LAN** and set up the **Management VLAN ID** (see Section 17.2.3 on page 207).

If no devices are in the management VLAN, then no one will be able to access the ZyXEL Device and you will have to restore the default configuration file.

4 Select the SSID profile you want to configure (**SSID03** in this example), and enter the **VLAN ID** number (between 1 and 4094).

5 Enter a **Second Rx VLAN ID**. The following screen shows **SSID03** tagged with a **VLAN ID** of **3** and a **Second Rx VLAN ID** of **4**.

Figure 137 Configuring SSID: Second Rx VLAN ID Example



6 Click **Apply** to save these settings. Outgoing packets from clients in **SSID03** are tagged with a **VLAN ID** of **3**, and incoming packets with a **VLAN ID** of **3** or **4** are forwarded to **SSID03**.

18

Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

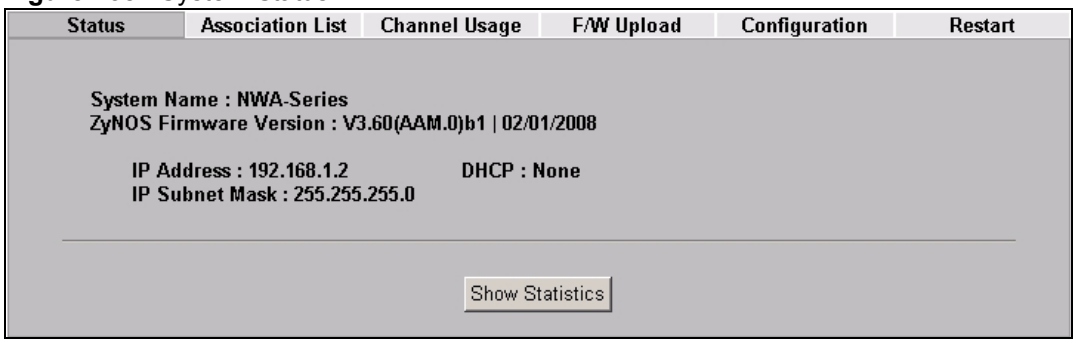
18.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyXEL Device.

18.2 System Status Screen

Click **MAINTENANCE** to open the **System Status** screen, where you can see information about your ZyXEL Device. Note that the labels in this screen are READ-ONLY and are meant to be used for diagnostic purposes.

Figure 138 System Status



The following table describes the labels in this screen.

Table 73 System Status

LABEL	DESCRIPTION
System Name	This is the **System Name** you can configure in the **SYSTEM** > **General** screen. It is for identification purposes
ZyNOS Firmware Version	This is the ZyNOS Firmware version and date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
IP Address	This is the Ethernet port IP address.
IP Subnet Mask	This is the Ethernet port subnet mask.

Table 73 System Status

LABEL	DESCRIPTION
DHCP	This is the Ethernet port DHCP role - **Client** or **None**.
Show Statistics	Click **Show Statistics** to see router performance statistics such as number of packets sent and number of packets received for each port.

18.2.1 System Statistics

Click **Maintenance > Show Statistics**. Read-only information here includes port status, packet specific statistics and bridge link status. Also provided are "system up time" and "poll interval(s)". The **Poll Interval** field is configurable. The fields in this screen vary according to the current wireless mode.

Figure 139 System Status: Show Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	7147	1417	0	3554	937	3:26:29
WLAN1	54M	6817	0	0	0	0	0:00:45
WLAN2	54M	6817	0	0	64	0	0:00:14

WLAN1:

Index	Active	Remote Bridge MAC	Status	TxPkts	RxPkts
1	No	00:00:00:00:00:00	Down	0	0
2	No	00:00:00:00:00:00	Down	0	0
3	No	00:00:00:00:00:00	Down	0	0
4	No	00:00:00:00:00:00	Down	0	0
5	No	00:00:00:00:00:00	Down	0	0

WLAN2:

Index	Active	Remote Bridge MAC	Status	TxPkts	RxPkts
1	No	00:00:00:00:00:00	Down	0	0
2	No	00:00:00:00:00:00	Down	0	0
3	No	00:00:00:00:00:00	Down	0	0
4	No	00:00:00:00:00:00	Down	0	0
5	No	00:00:00:00:00:00	Down	0	0

Poll Interval(s) : 5 sec Set Interval Stop

The following table describes the labels in this screen.

Table 74 System Status: Show Statistics

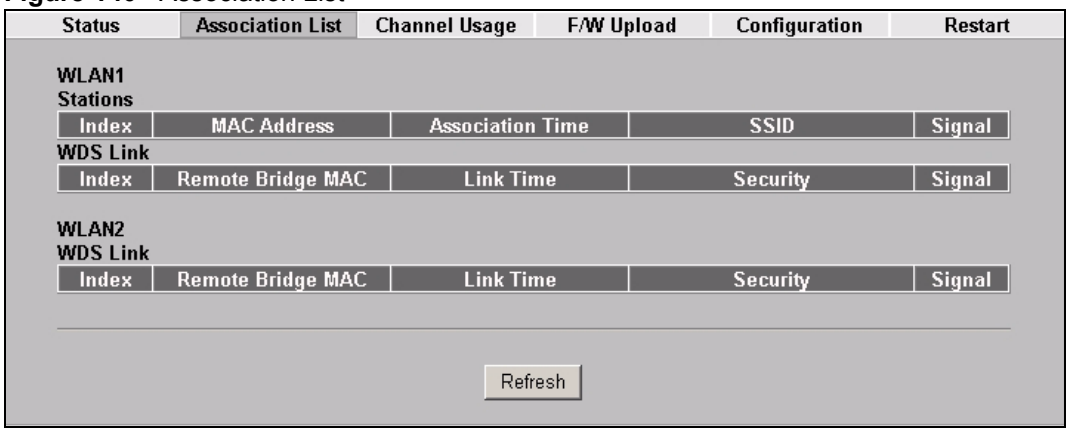
LABEL	DESCRIPTION
Port	This is the Ethernet port (**LAN**) or wireless LAN adaptor (**WLAN1** or **WLAN2**).
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect. This shows the transmission speed only for the wireless adaptors.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This shows the transmission speed in bytes per second on this port.
Rx B/s	This shows the reception speed in bytes per second on this port.
Up Time	This is total amount of time the line has been up.
WLAN1	This section displays only when wireless LAN adaptor WLAN1 is in **AP+Bridge** or **Bridge/Repeater** mode.
WLAN2	This section displays only when wireless LAN adaptor WLAN2 is in **AP+Bridge** or **Bridge/Repeater** mode.
Index	This is the index number of the bridge connection.
Remote Bridge MAC	This is the MAC address of the peer device in bridge mode.
Status	This shows the current status of the bridge connection, which can be **Up** or **Down**.
TxPkts	This is the number of transmitted packets on the wireless bridge.
RxPkts	This is the number of received packets on the wireless bridge.
Poll Interval(s)	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.
Stop	Click this button to stop refreshing statistics.

18.3 Association List

View the wireless stations that are currently associated with the ZyXEL Device in the **Association List** screen.

Click **MAINTENANCE** > **Association List** to display the screen as shown next.

Figure 140 Association List



The following table describes the labels in this screen.

Table 75 Association List

LABEL	DESCRIPTION
Stations	
Index	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
SSID	This field displays the SSID to which the wireless station is associated.
Signal	This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection.
WDS Link	This section displays only when bridge mode is activated on one of the ZyXEL Device's WLAN adaptors.
Index	This field displays the index number of a bridge connection on the WDS.
Remote Bridge MAC	This field displays a remote bridge MAC address.
Link Time	This field displays the WDS link up-time.
Security	This field displays whether traffic on the WDS is encrypted (**TKIP** or **AES**) or not (**None**).
Refresh	Click **Refresh** to reload the screen.

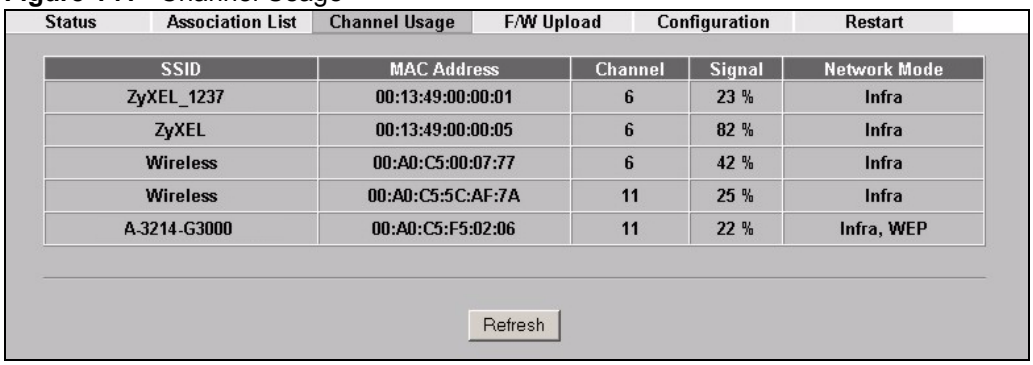
18.4 Channel Usage

The **Channel Usage** screen shows whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.

Click **MAINTENANCE** > **Channel Usage** to display the screen shown next.

Wait a moment while the ZyXEL Device compiles the information.

Figure 141 Channel Usage



The following table describes the labels in this screen.

Table 76 Channel Usage

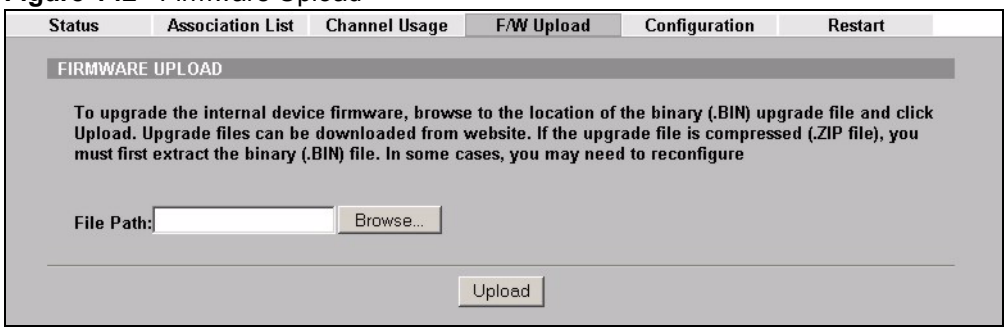
LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the chapter on wireless configuration for more information on basic service sets (BSS) and extended service sets (ESS).
MAC Address	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Signal	This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference.
Network Mode	"Network mode" in this screen refers to your wireless LAN infrastructure (refer to the Wireless LAN chapter) and security setup.
Refresh	Click **Refresh** to reload the screen.

18.5 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, for example "NWA-Series.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** > **F/W Upload**. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 142 Firmware Upload



The following table describes the labels in this screen.

Table 77 Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

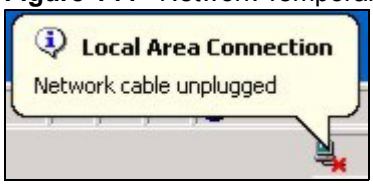
Do not turn off the ZyXEL Device while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 143 Firmware Upload In Process

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 144 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

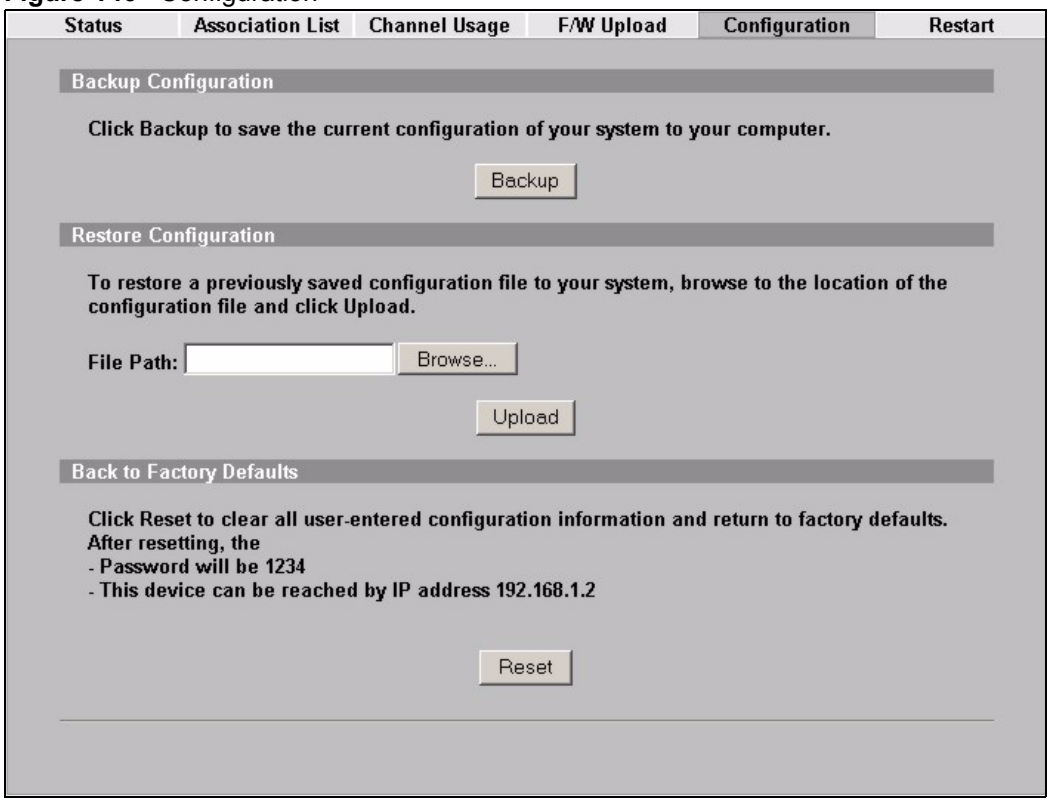
Figure 145 Firmware Upload Error

18.6 Configuration Screen

See Chapter 24 on page 251 for information on how to transfer configuration files using FTP/TFTP commands.

Click **MAINTENANCE** > **Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 146 Configuration



18.6.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

18.6.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

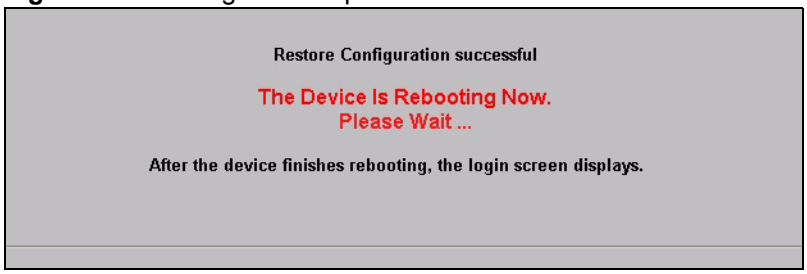
Table 78 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

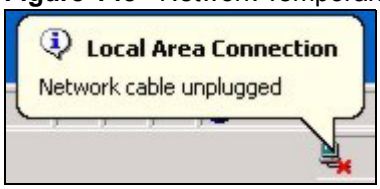
After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 147 Configuration Upload Successful



The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 148 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.2). See your Quick Start Guide for details on how to set up your computer’s IP address.

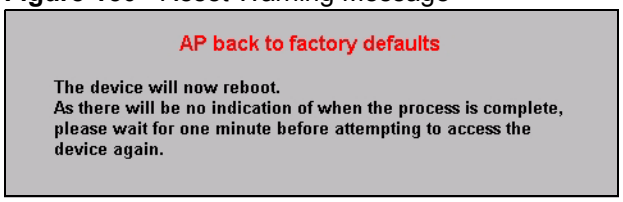
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 149 Configuration Upload Error

18.6.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 150 Reset Warning Message



You can also press the **RESET** button to reset your ZyXEL Device to its factory default settings. Refer to Section 2.2 on page 44 for more information.

18.7 Restart Screen

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **MAINTENANCE** > **Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 151 Restart Screen

PART III
Troubleshooting and Specifications

Troubleshooting (233)
Product Specifications (237)

19

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power and Hardware Connections
- ZyXEL Device Access and Login
- Internet Access
- Wireless Router/AP Troubleshooting

19.1 Power and Hardware Connections

The ZyXEL Device does not turn on.

1. Make sure you are using the PoE power injector included with the ZyXEL Device.
2. Make sure the PoE power injector is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the PoE power injector to the ZyXEL Device.
4. If the problem continues, contact the vendor.

19.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1. The default IP address is **192.168.1.2**.
2. If you changed the static IP address and have forgotten it, you have to reset the device to its factory defaults. Contact your vendor.

   If you set the ZyXEL Device to get a dynamically assigned IP address from a DHCP server, check your DHCP server for the IP address assigned to the ZyXEL Device.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. Contact your vendor.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.2.
   - If you changed the IP address (Section 11.3 on page 142), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.
2. Check the hardware connections. See the Quick Start Guide.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Section 19.1 on page 233.
4. Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device.
5. Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. Contact your vendor.
6. If the problem continues, contact the network administrator or vendor, or try the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings to find out why the ZyXEL Device does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1. Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
2. You cannot log in to the web configurator while someone is using the SMT or Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.
3. Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.

4 If this does not work, you have to reset the device to its factory defaults. Contact your vendor.

I cannot access the SMT.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

19.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the ZyXEL Device is connected to a broadband modem or router that provides Internet access. See the Quick Start Guide.
2 Make sure your Internet account is activated and you entered your ISP account information correctly in the broadband modem or router to which the ZyXEL Device is connected. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3 If you are trying to access the Internet wirelessly, make sure the wireless settings on the wireless client are the same as the settings on the AP.
4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1 Check the hardware connections. See the Quick Start Guide.
2 Reboot the ZyXEL Device.
3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Make sure the ZyXEL Device is installed in a position free of obstructions.
3. Check the signal strength. If the signal is weak, try moving your computer closer to the ZyXEL Device (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).
4. Reboot the ZyXEL Device.
5. If the problem continues, contact the network administrator or vendor, or try the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

19.4 Wireless Router/AP Troubleshooting

I cannot access the ZyXEL Device or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the ZyXEL Device
2. Make sure the wireless adapter on the wireless client is working properly.
3. Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the ZyXEL Device.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the ZyXEL Device.
5. Check that both the ZyXEL Device and your wireless client are using the same wireless and wireless security settings.
6. Make sure you allow the ZyXEL Device to be remotely accessed through the WLAN interface. Check your remote management settings.

20

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Table 79 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	256 (W) x 246 (D) x 82 (H) mm
Weight	2000 g
Power	PoE draw: 48V 20W at least
Ethernet Port	Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
Power over Ethernet (PoE)	IEEE 802.3af compliant.
Antenna Specifications	Two external antenna connectors (N-Type).
Output Power	IEEE 802.11b/g: 17 dBm IEEE 802.11a: 14 dBm
Operating Environment	Temperature: -35º C ~ 55º C Humidity: 10% ~ 90% RH

Table 79 Hardware Specifications

SPECIFICATION	DESCRIPTION
Storage Environment	Temperature: -40º C ~ 60º C Humidity: 5% ~ 95% RH
Approvals	Radio • USA: FCC Part 15C 15.247 FCC Part 15E 15.407 FCC OET65 • EU: ETSI EN 300 328 V1.7.1 ETSI EN 301 893 V1.2.3 • Taiwan: DGT LP0002 • Canada: Industry Canada RSS-210 • Australia: AS/NZS 4268 EMC/ EMI • USA: FCC Part 15 Subpart B • EU: EN 301 489-17 V1.2.1: 08-2002 EN 55022:2006 • Canada: ICES-003 • Australia: AS/NZS CISPR22 EMC/ EMS • EU: EN 301 489-1 V1.5.1: 11-2004 Environmental • 2002/95/EC (RoHS) Restriction of Hazardous Substances Directive • 2002/96/EC (WEEE) Waste Electrical and Electronic Equipment Directive • European Parliament and Council Directive 94/62/EC of 20 December 1994 on packaging and packaging waste

Table 80 Firmware Specifications

Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Wireless LAN Standards	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g
Wireless security	WEP, WPA(2), WPA(2)-PSK, IEEE 802.1x
Layer 2 isolation	Prevents wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.
Multiple BSSID (MBSSID)	MBSSID mode allows the ZyXEL Device to operate up to 8 different wireless networks (BSSs) simultaneously, each with independently-configurable wireless and security settings.
Rogue AP detection	Rogue AP detection detects and logs unknown access points (APs) operating in the area.
Internal RADIUS server	PEAP, 32-entry Trusted AP list, 128-entry Trusted Users list.
VLAN	802.1Q VLAN tagging.

Table 80 Firmware Specifications

STP (Spanning Tree Protocol) / RSTP (Rapid STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network.
WMM QoS	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic.
Certificates	The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.
SSL Passthrough	SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https” instead of “http”. The ZyXEL Device allows SSL connections to take place through the ZyXEL Device.
MAC Address Filter	Your ZyXEL Device checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.
Wireless Association List	With the wireless association list, you can see the list of the wireless stations that are currently using the ZyXEL Device to access your wired network.
Logging and Tracing	Built-in message logging and packet tracing.
Embedded FTP and TFTP Servers	The embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.
Auto Configuration	Administrators can use text configuration files to configure the wireless LAN settings for multiple APs. The AP can automatically get a configuration file from a TFTP server at start up or after renewing DHCP client information.
SNMP	SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manger station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The NWA-3165 also supports version 3 (SNMPv3).
DFS	DFS (Dynamic Frequency Selection) allows a wider choice of 802.11a wireless channels.
CAPWAP (Control and Provisioning of Wireless Access Points)	The ZyXEL Device can be managed via CAPWAP, which allows multiple APs to be configured and managed by a single AP controller.

Compatible ZyXEL Antennas

At the time of writing, you can use the following antennas in your ZyXEL Device.

Table 81 ZyXEL Device Compatible Antennas

MODEL / FEATURES	EXT-108	EXR-109	EXT-114	EXT-118	ANT2206		ANT3108	ANT3218
Frequency Band (MHz)	2400 ~ 2500	2400 ~ 2500	2400 ~ 2500	2400 ~ 2500	2400 ~ 2500	4900 ~ 5875	5150 ~ 5875	4900 ~ 5875
Gain (dBi)	8	9	14	18	6	8	8	18
Max. VSWR	2.0:1	1.5:1	1.5:1	1.5:1	2.0:1	2.0:1	2.0:1	2.0:1
HPBW/ Horizontal	360º	65º	30º	15º	65º	50º	360º	18º
HPBW/ Vertical	15º	60º	30º	5º	75º	50º	20º	18º
Impedance (Ohm)	50	50	50	50	50		50	50
Connector	N type female	N type female	N type female	N type female	RP SMA plug		N type female	N type female
Survival Wind Speed (km/hr)	216	216	216	180			216	216
Temperature	-40ºC ~ 80ºC	-40ºC ~ 80ºC	-40ºC ~ 80ºC	-40ºC ~ 80ºC	-10ºC ~ 55ºC		-40ºC ~ 80ºC	-40ºC ~ 80ºC
Humidity	95% at 25ºC	95% at 55ºC	95% at 55ºC	95% at 55ºC	95% at 55ºC		95% at 55ºC	95% at 55ºC
Weight	337 gw	107 gw	407 g	1.6 kg	110 g		206 g	640 gw

Compatible ZyXEL Antenna Cables

The following table shows you the cables you can use in the ZyXEL Device to extend your connection to antennas at the time of writing.

Table 82 ZyXEL Device Compatible Antenna Cables

MODEL NAME	PART NUMBER (P/N)	LENGTH
LMR-400	91-005-075001G	N-PLUG to N-PLUG, for 6M
	91-005-075002G	N-PLUG to N-PLUG, for 9M
	91-005-075003G	N-PLUG to N-PLUG, for 12M
	91-005-075004G	N-PLUG to N-PLUG, for 1M
LMR-200	91-005-074001G	N-PLUG to RP-SMA PLUG, for 3M
	91-005-074002G	N-PLUG to RP-SMA PLUG, for 6M
	91-005-074003G	N-PLUG to RP-SMA PLUG, for 9M
EXT-300	91-005-082001B	Jumper Cable, Surge Arrstor

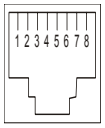
Power over Ethernet (PoE) Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.

Table 83 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Table 84 Power over Ethernet Injector RJ-45 Port Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

PART IV Appendices and Index

Setting Up Your Computer's IP Address (245)
Wireless LANs (269)
Pop-up Windows, JavaScripts and Java Permissions (283)
Importing Certificates (289)
IP Addresses and Subnetting (313)
Text File Based Auto Configuration (321)
Legal Information (329)
Customer Support (333)
Index (339)

A

Setting Up Your Computer's IP Address

Your specific ZyXEL device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

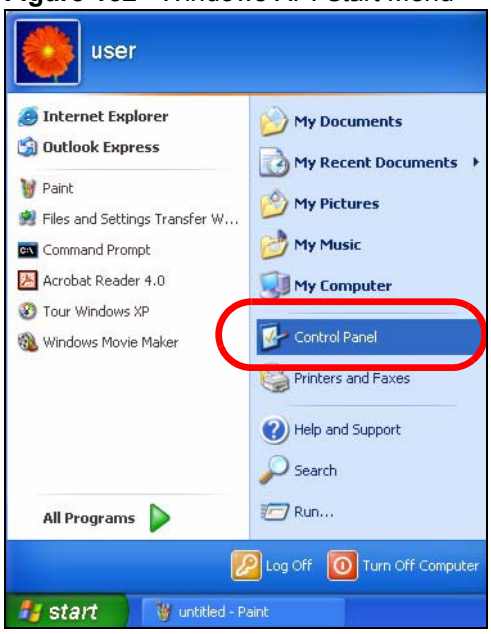
- Windows XP/NT/2000 on page 245
- Windows Vista on page 248
- Mac OS X: 10.3 and 10.4 on page 252
- Mac OS X: 10.5 on page 256
- Linux: Ubuntu 8 (GNOME) on page 259
- Linux: openSUSE 10.3 (KDE) on page 262

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

Figure 152 Windows XP: Start Menu

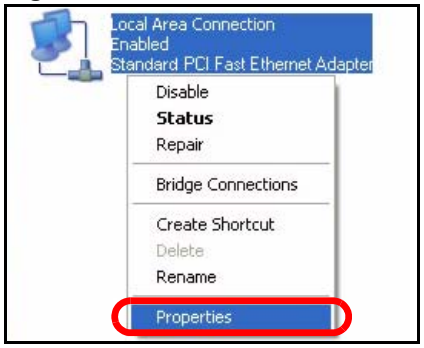


2 In the **Control Panel**, click the **Network Connections** icon.

Figure 153 Windows XP: Control Panel

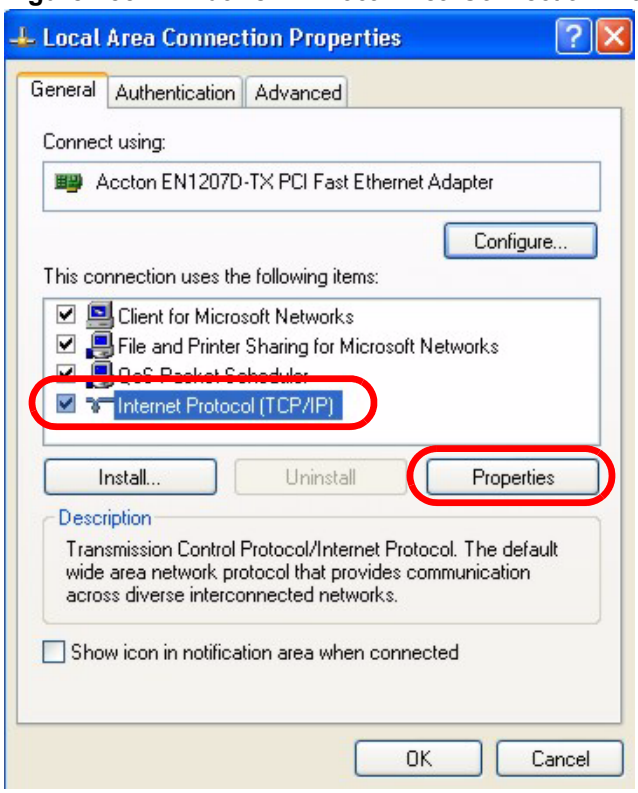
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 154 Windows XP: Control Panel > Network Connections > Properties



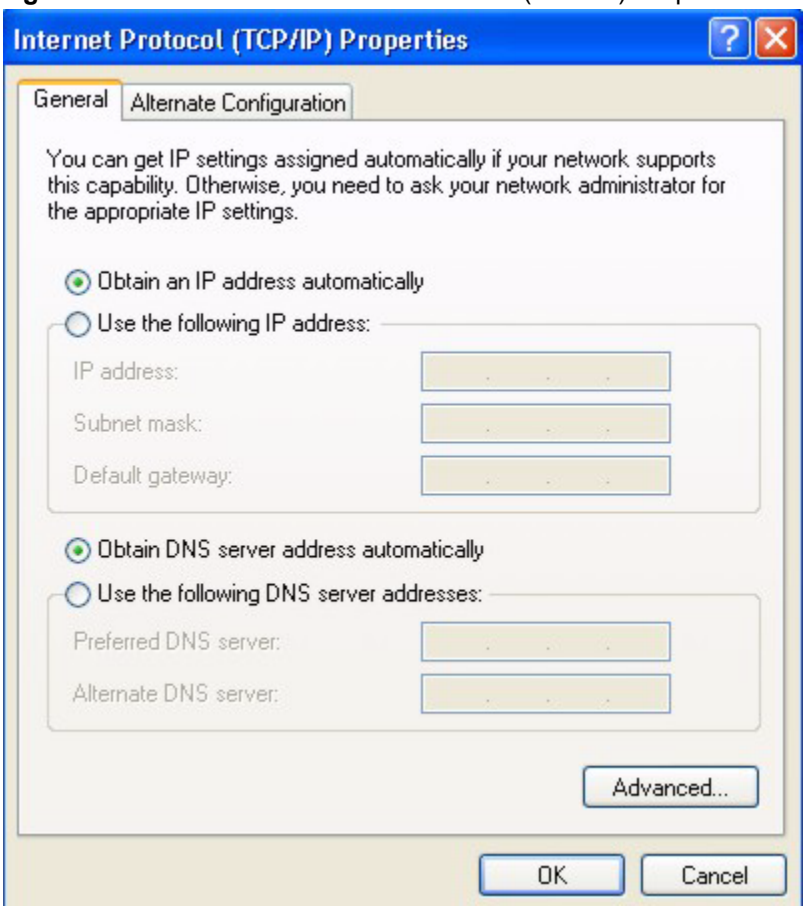
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 155 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 156 Windows XP: Internet Protocol (TCP/IP) Properties



6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

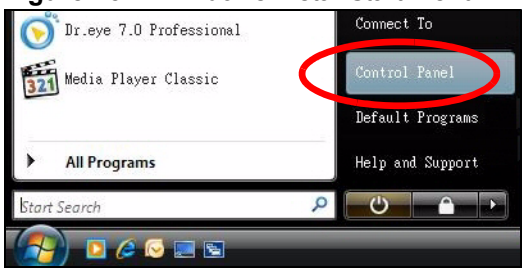
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

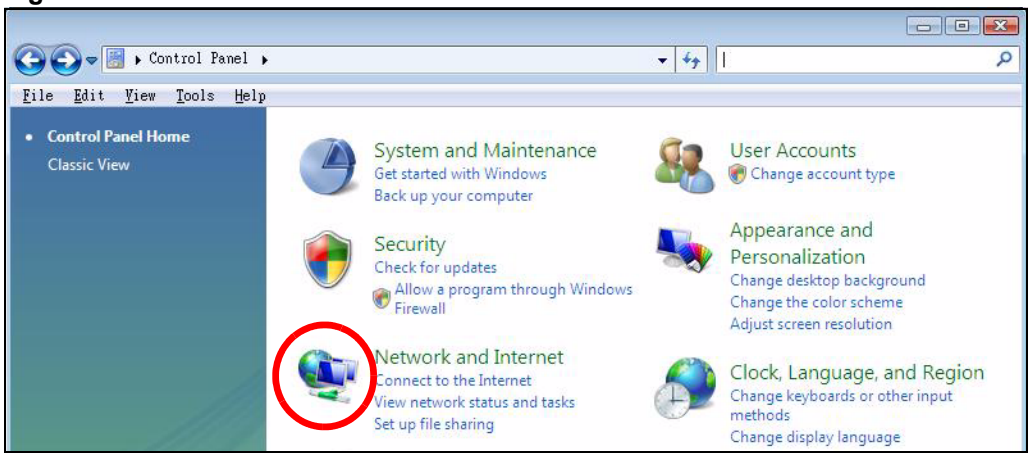
1 Click **Start** > **Control Panel**.

Figure 157 Windows Vista: Start Menu



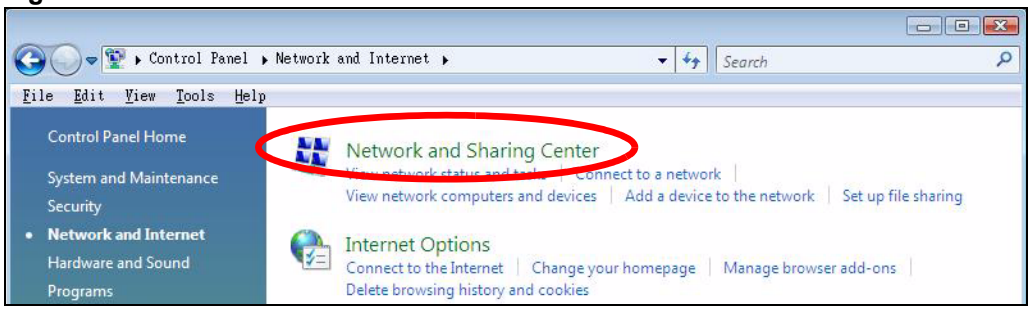
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 158 Windows Vista: Control Panel



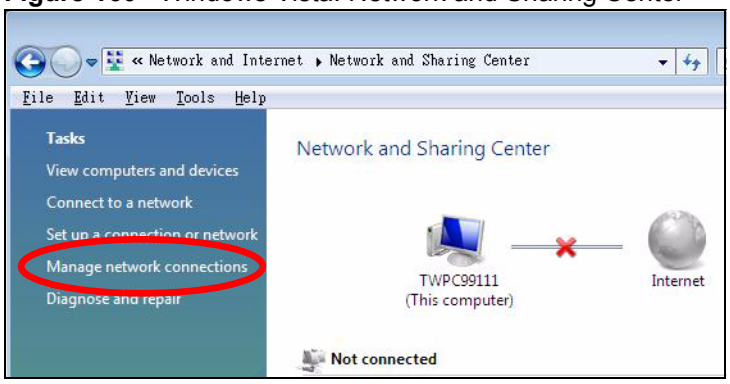
3 Click the **Network and Sharing Center** icon.

Figure 159 Windows Vista: Network And Internet



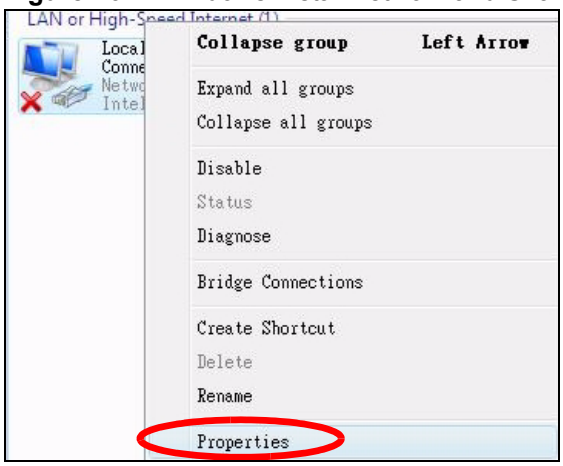
4 Click **Manage network connections**.

Figure 160 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

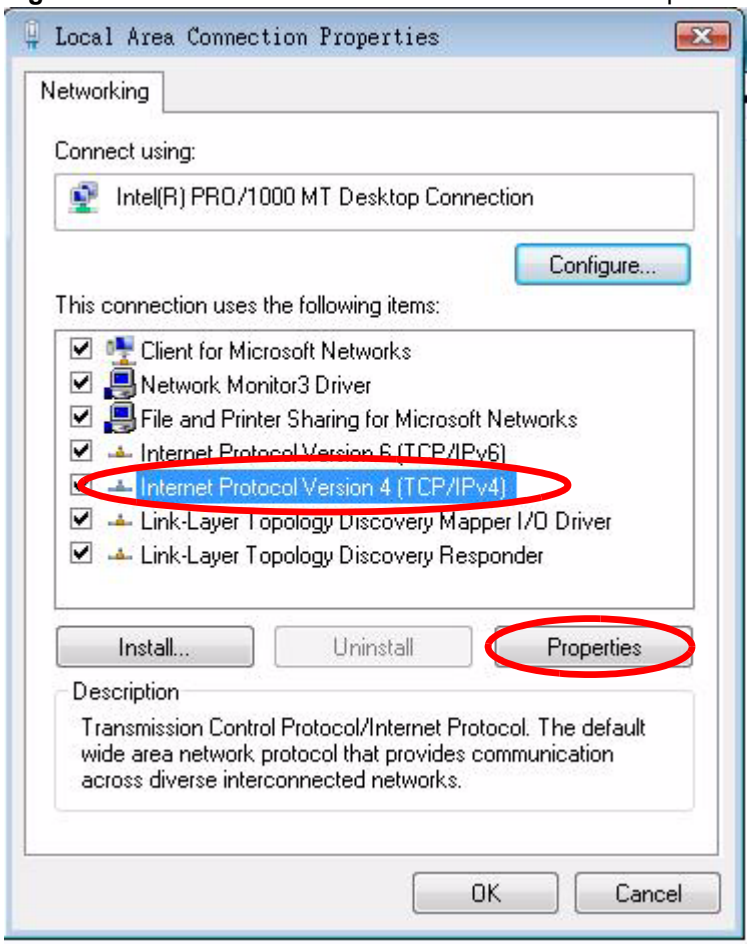
Figure 161 Windows Vista: Network and Sharing Center



During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

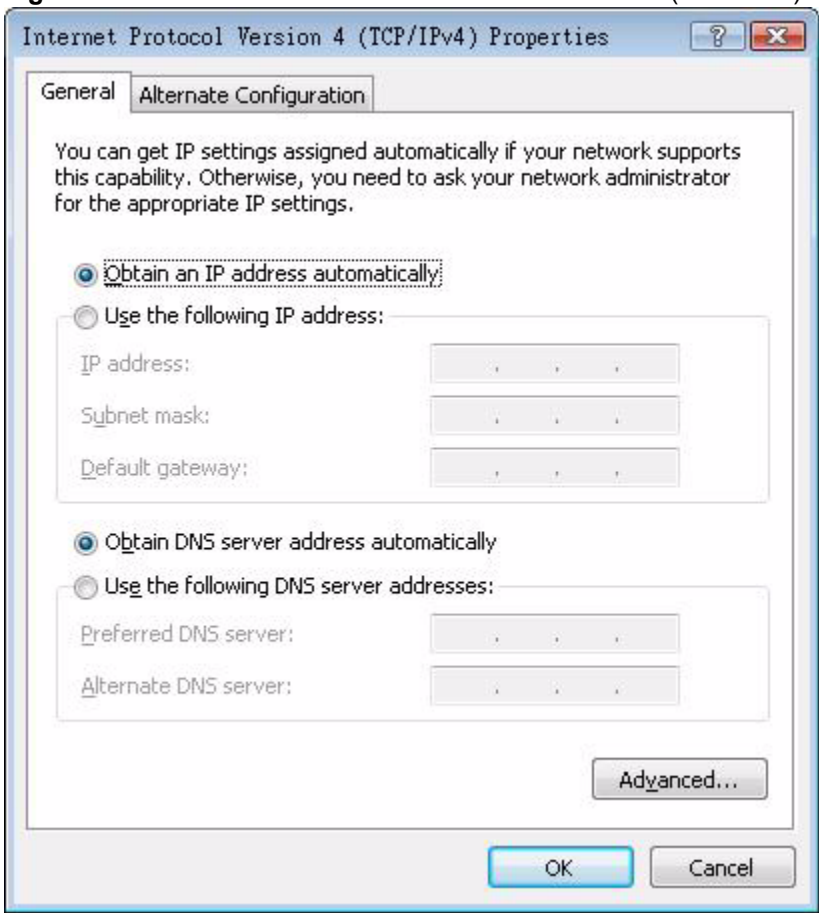
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 162 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 163 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

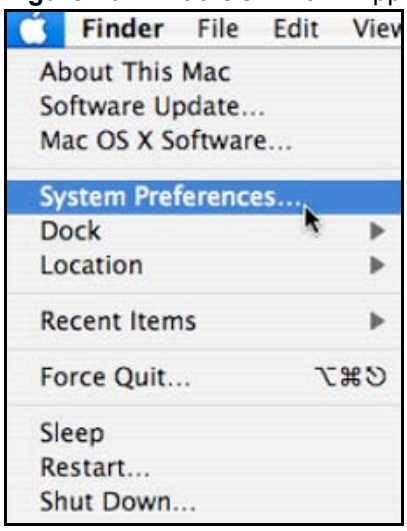
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

Figure 164 Mac OS X 10.4: Apple Menu

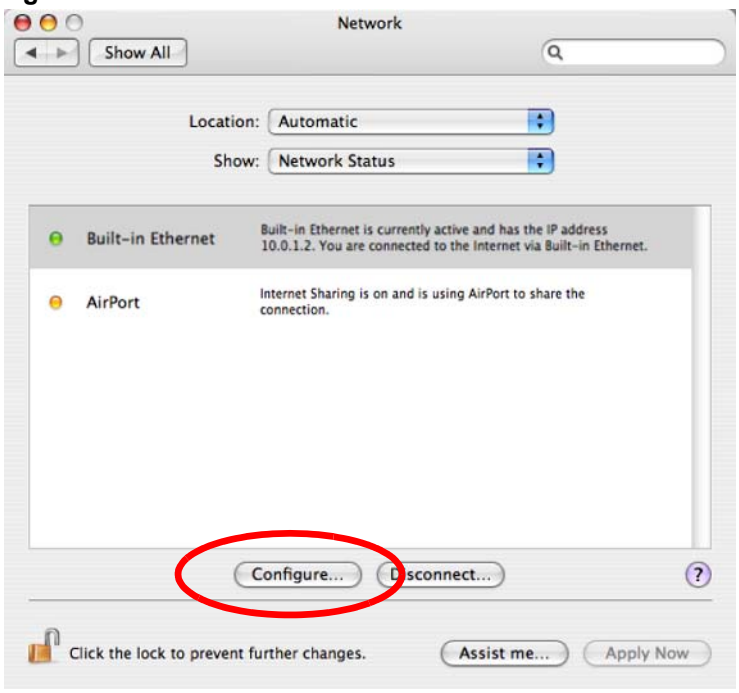


2 In the **System Preferences** window, click the **Network** icon.

Figure 165 Mac OS X 10.4: System Preferences

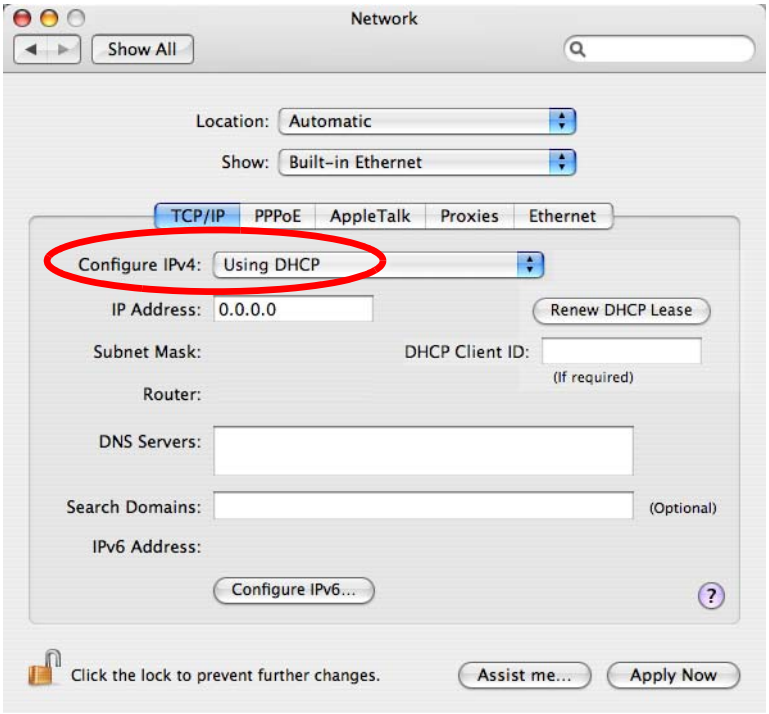
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 166 Mac OS X 10.4: Network Preferences



4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 167 Mac OS X 10.4: Network Preferences > TCP/IP Tab.

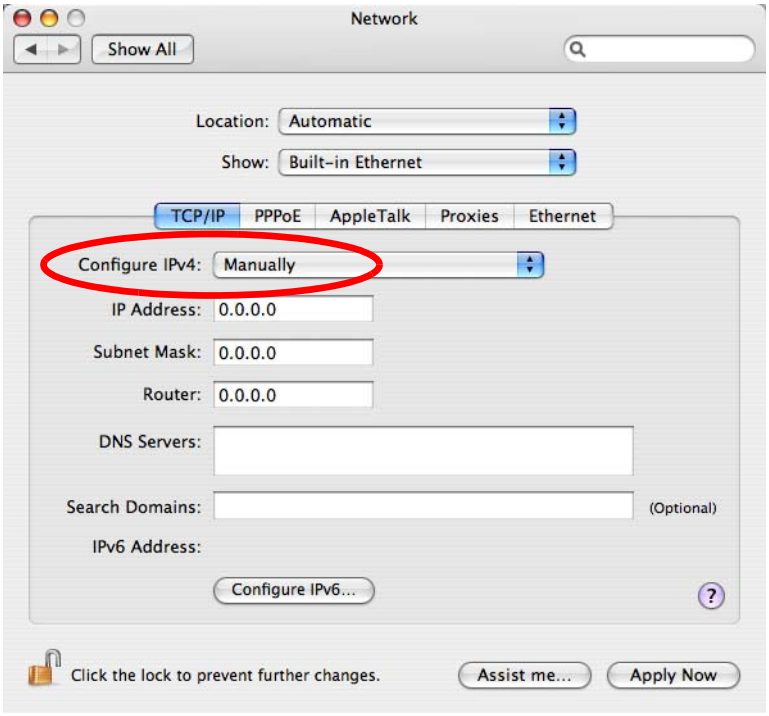


5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.

- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

Figure 168 Mac OS X 10.4: Network Preferences > Ethernet

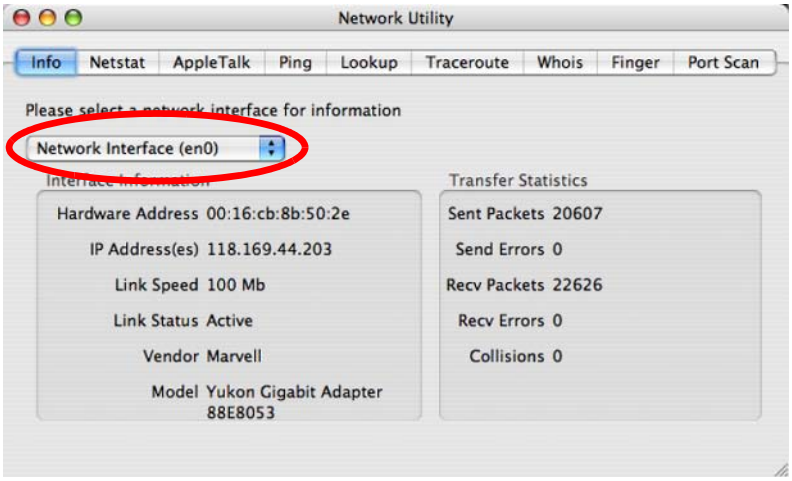


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 169 Mac OS X 10.4: Network Utility

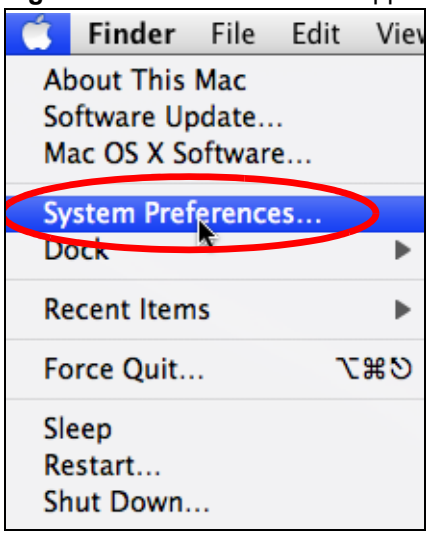


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

Figure 170 Mac OS X 10.5: Apple Menu

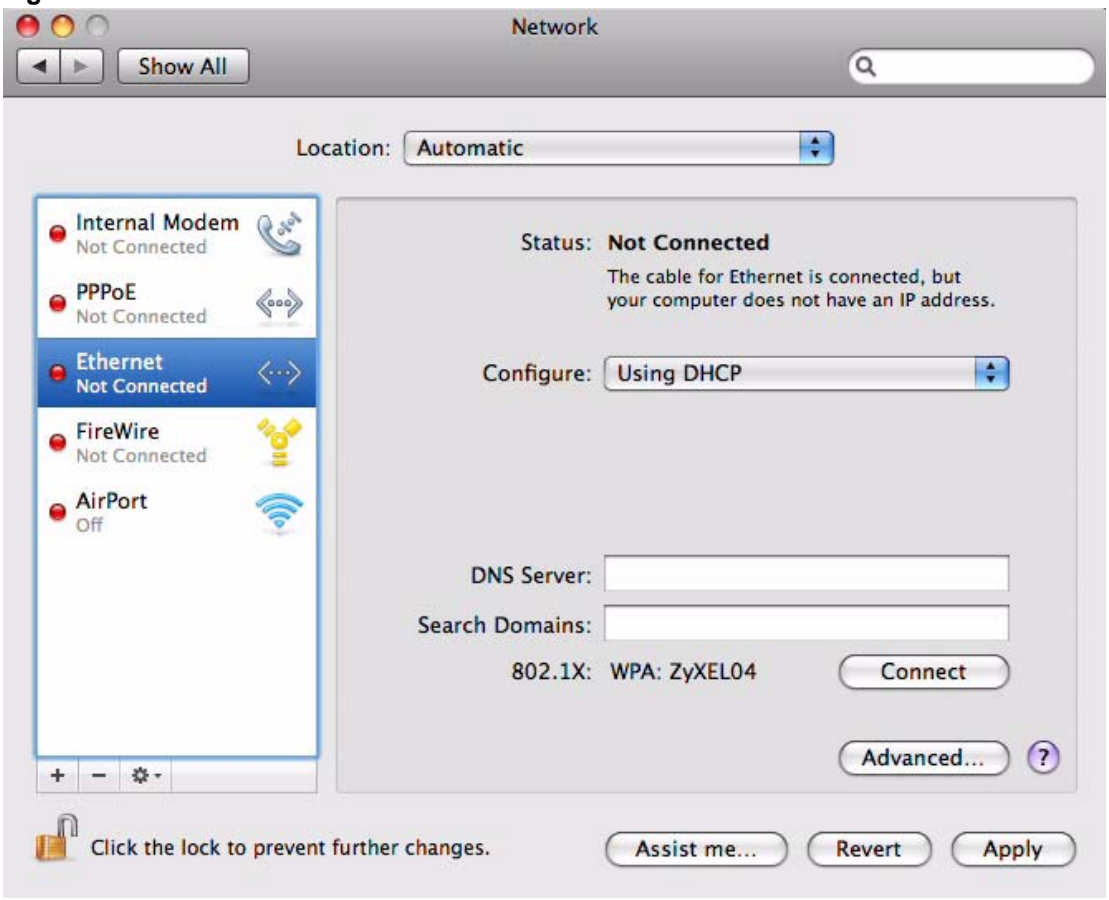


2 In **System Preferences**, click the **Network** icon.

Figure 171 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 172 Mac OS X 10.5: Network Preferences > Ethernet

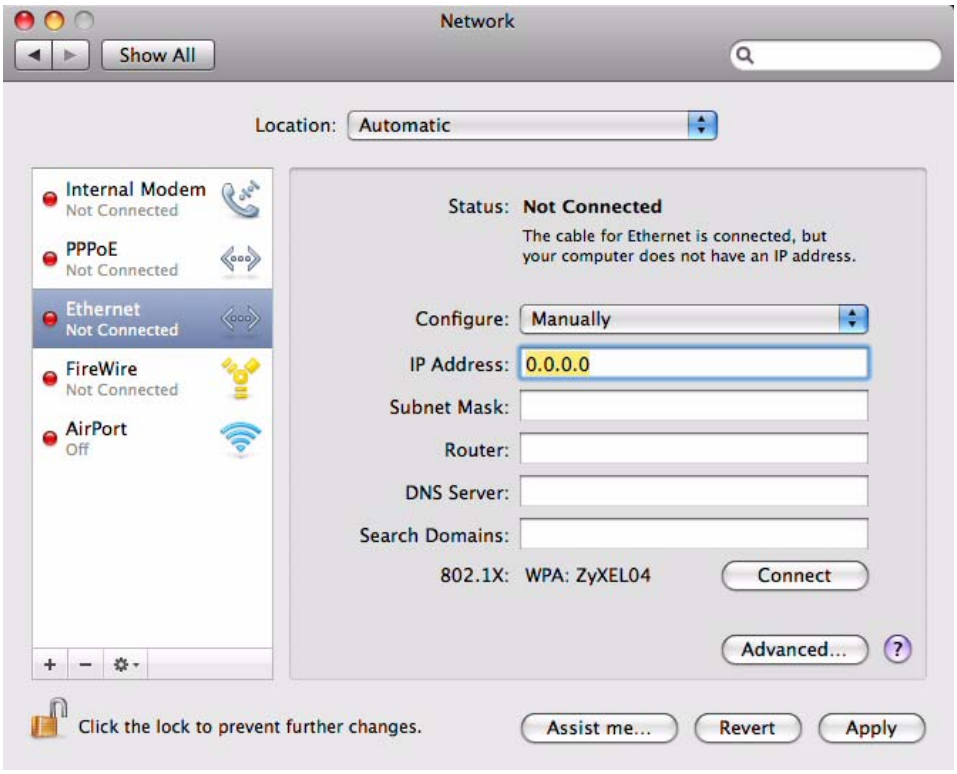


4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your ZyXEL Device.

Figure 173 Mac OS X 10.5: Network Preferences > Ethernet

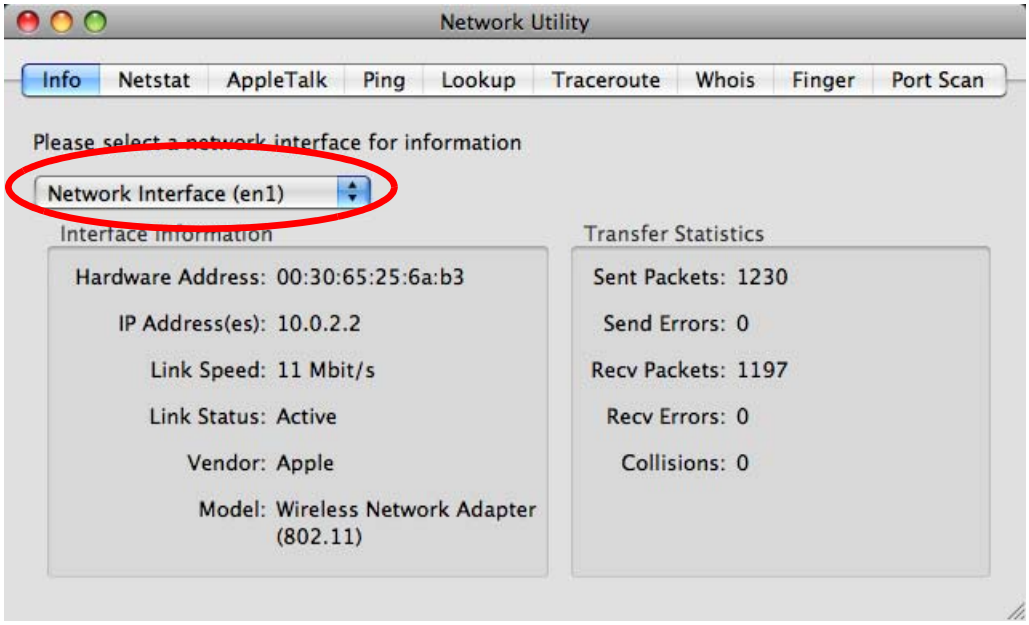


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 174 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

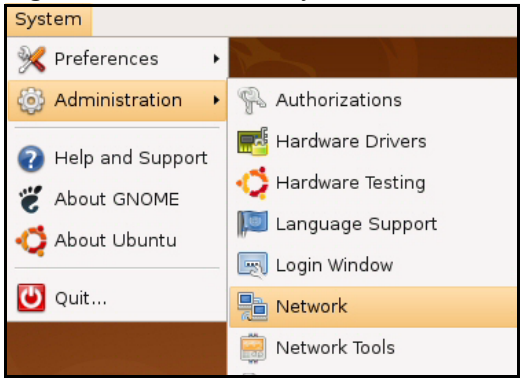
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

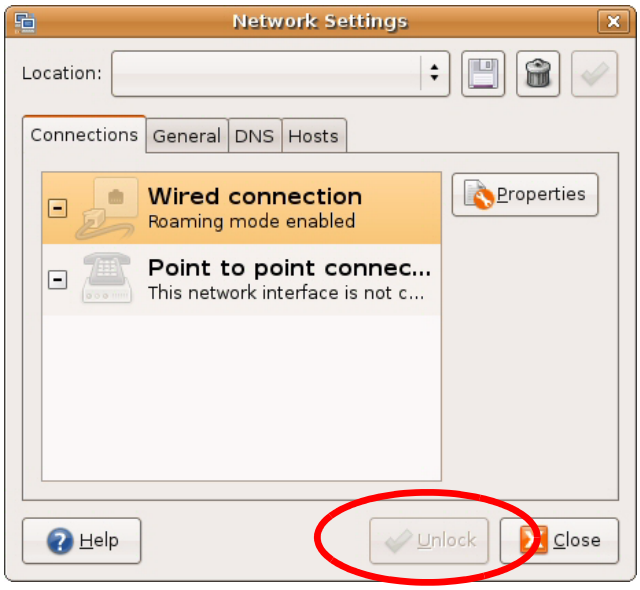
1 Click **System > Administration > Network**.

Figure 175 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 176 Ubuntu 8: Network Settings > Connections



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

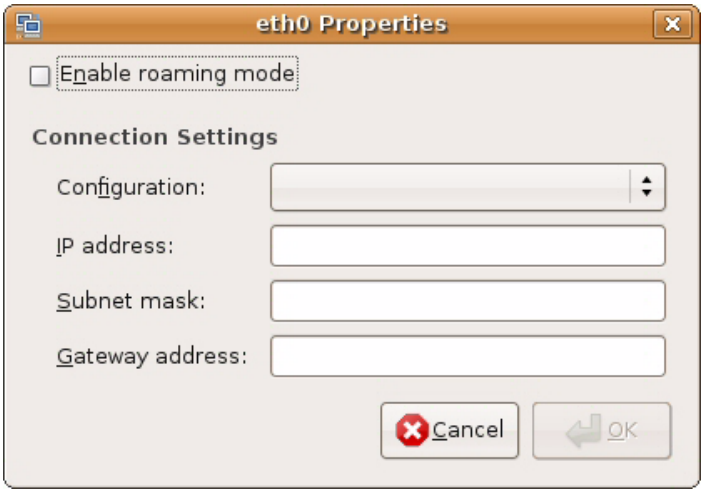
Figure 177 Ubuntu 8: Administrator Account Authentication

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 178 Ubuntu 8: Network Settings > Connections

5 The **Properties** dialog box opens.

Figure 179 Ubuntu 8: Network Settings > Properties

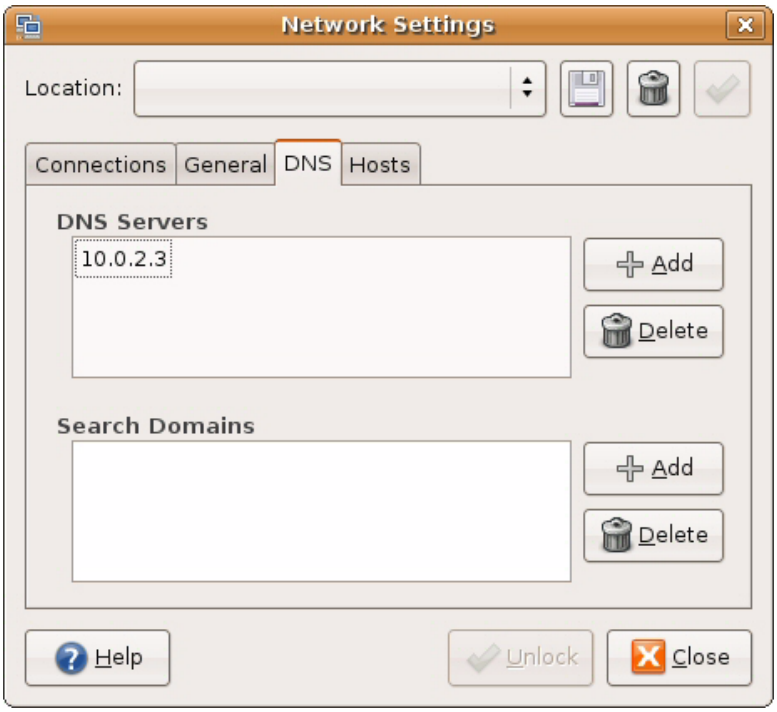


- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 180 Ubuntu 8: Network Settings > DNS

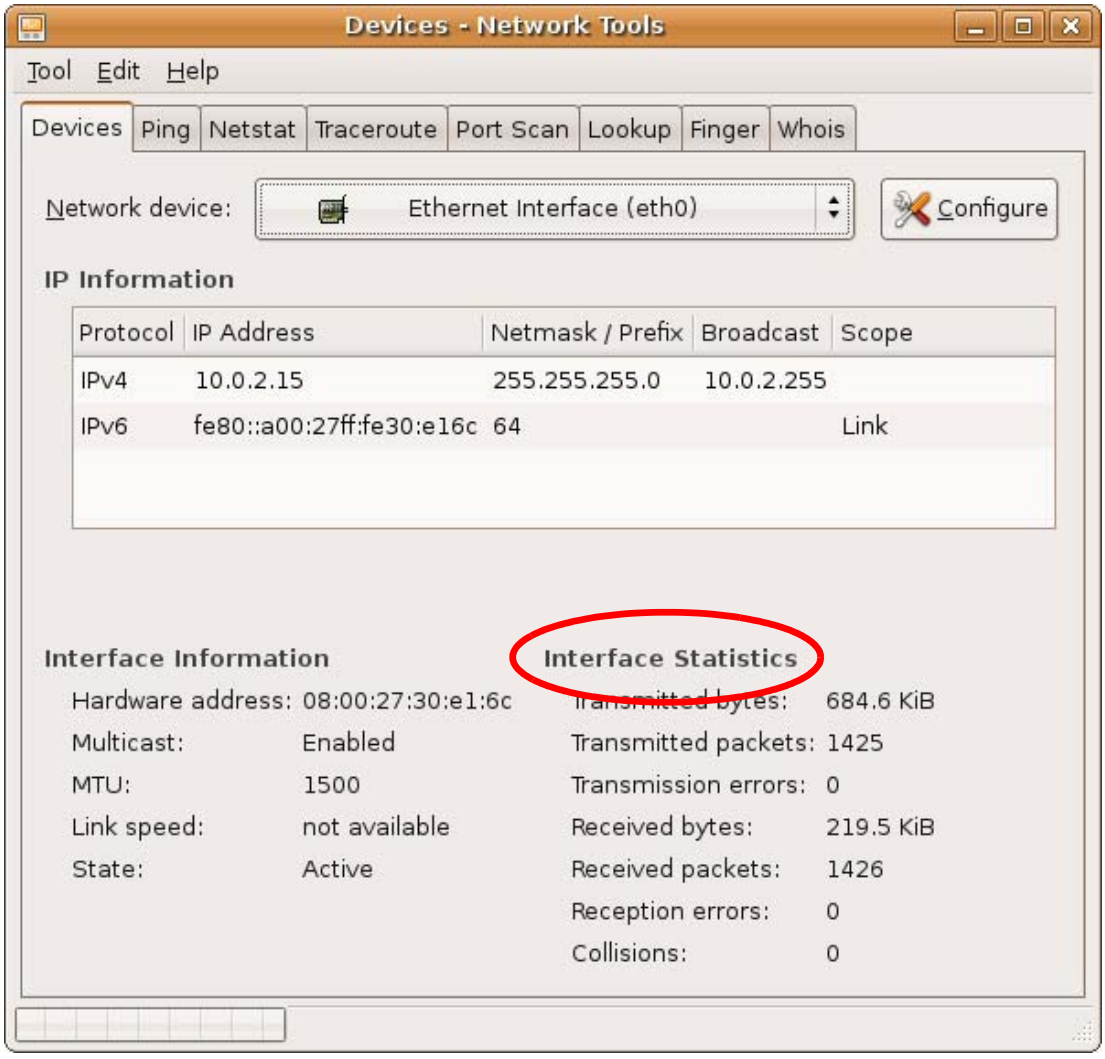


8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 181 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

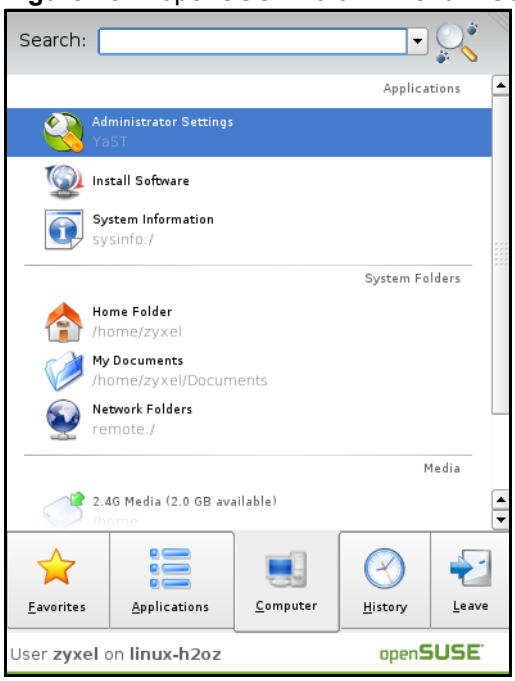
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

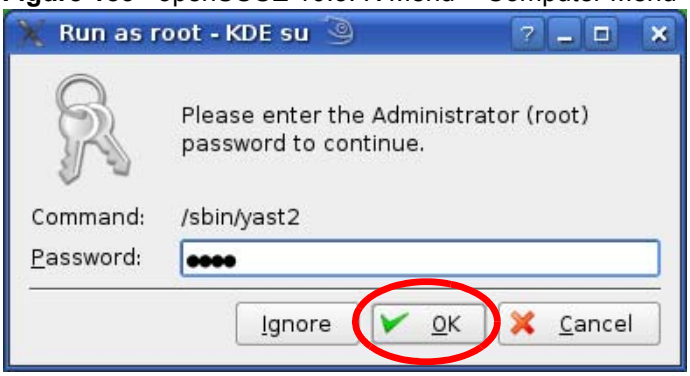
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 182 openSUSE 10.3: K Menu > Computer Menu



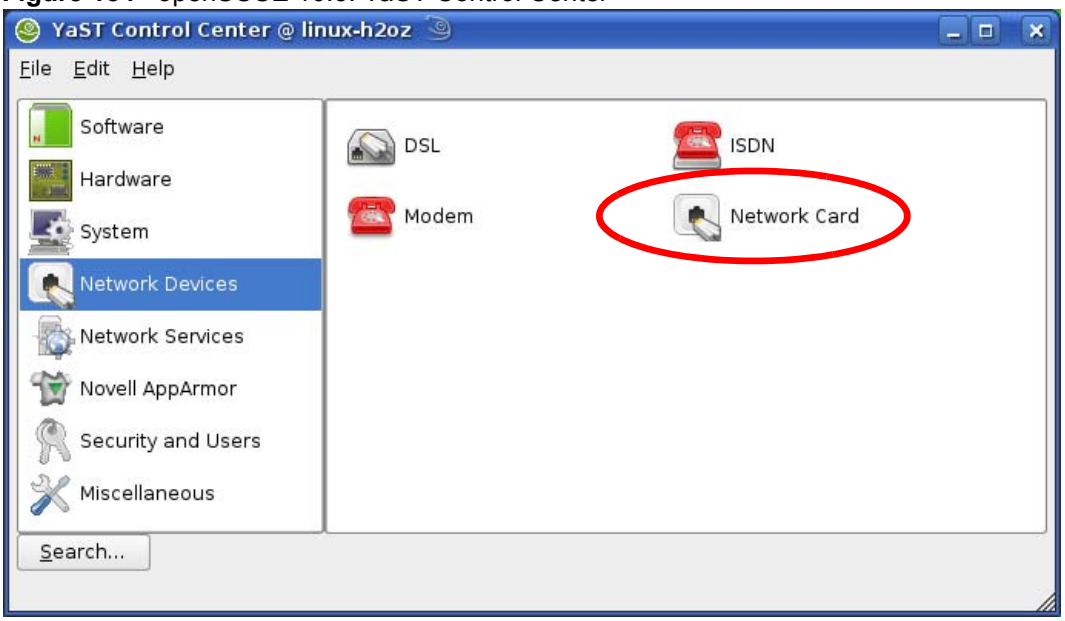
2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 183 openSUSE 10.3: K Menu > Computer Menu



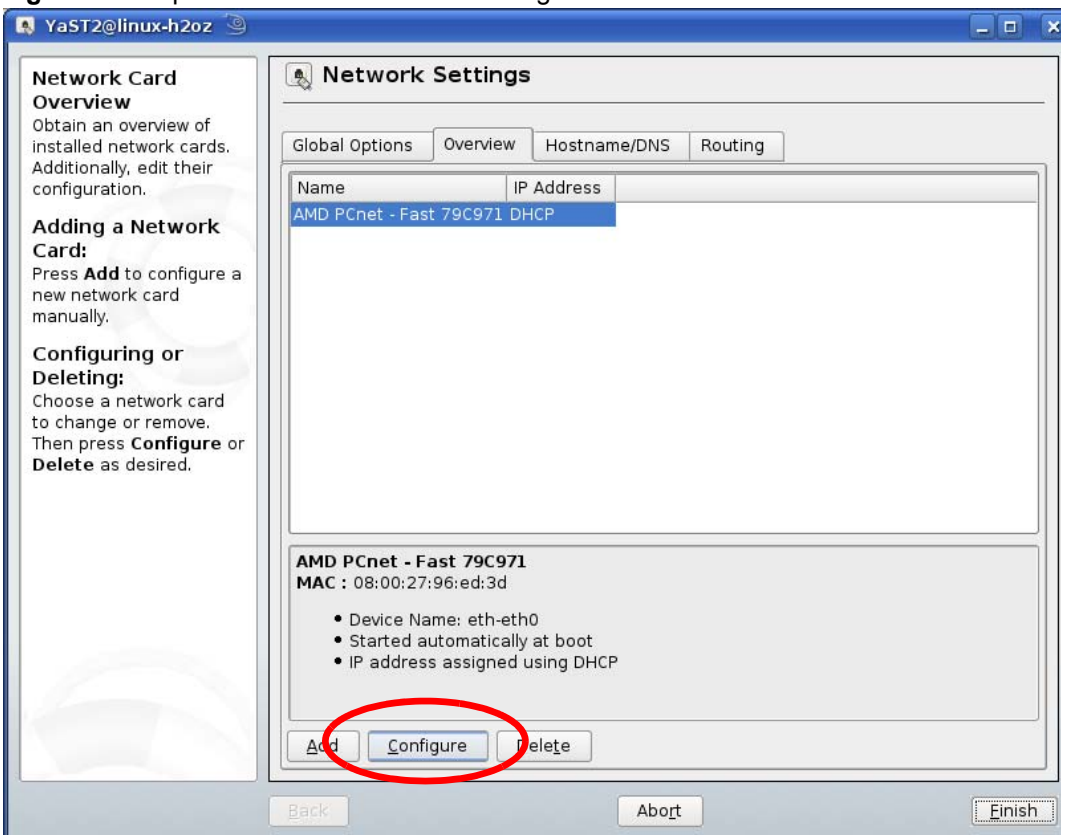
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 184 openSUSE 10.3: YaST Control Center



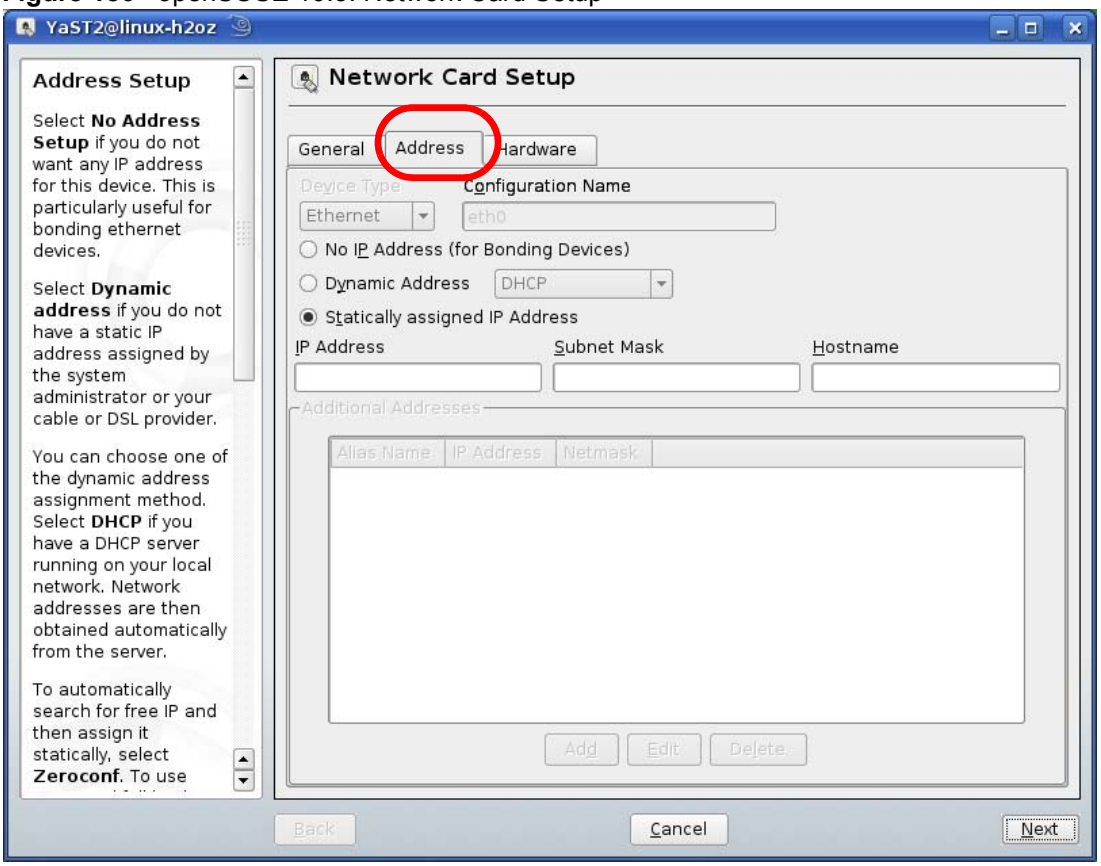
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 185 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 186 openSUSE 10.3: Network Card Setup

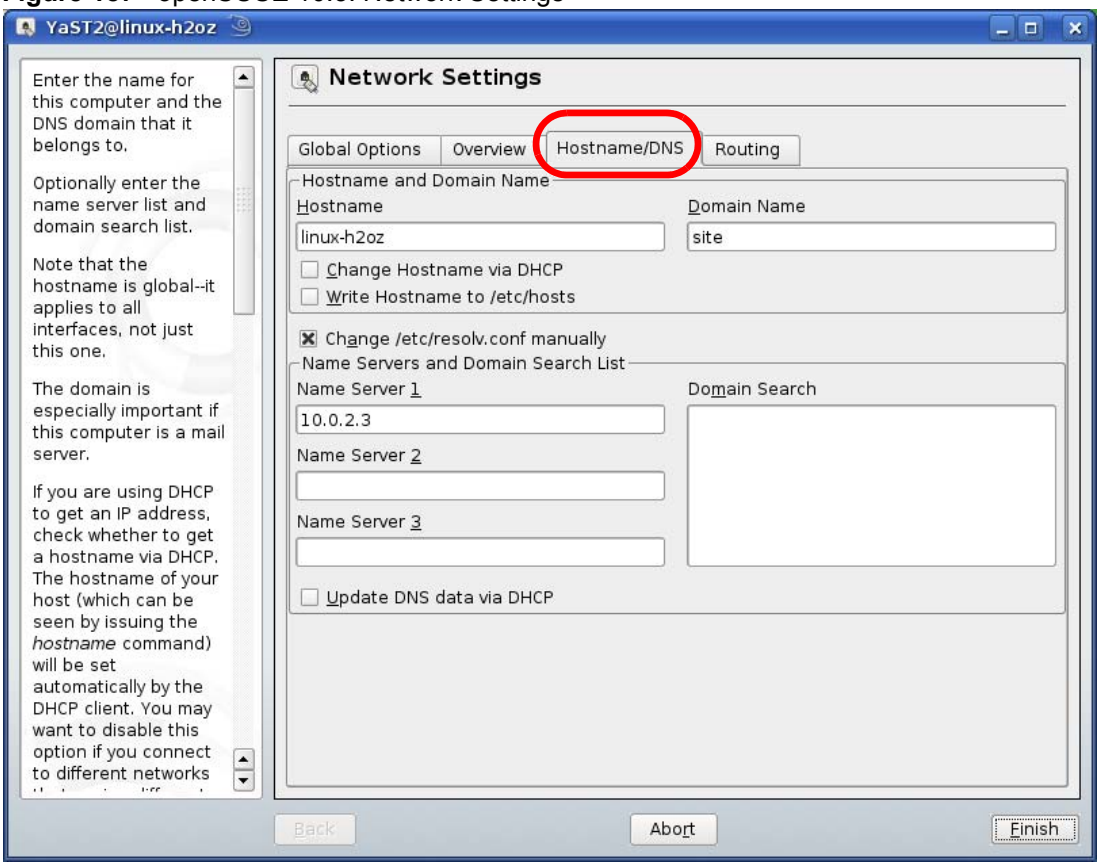


6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 187 openSUSE 10.3: Network Settings

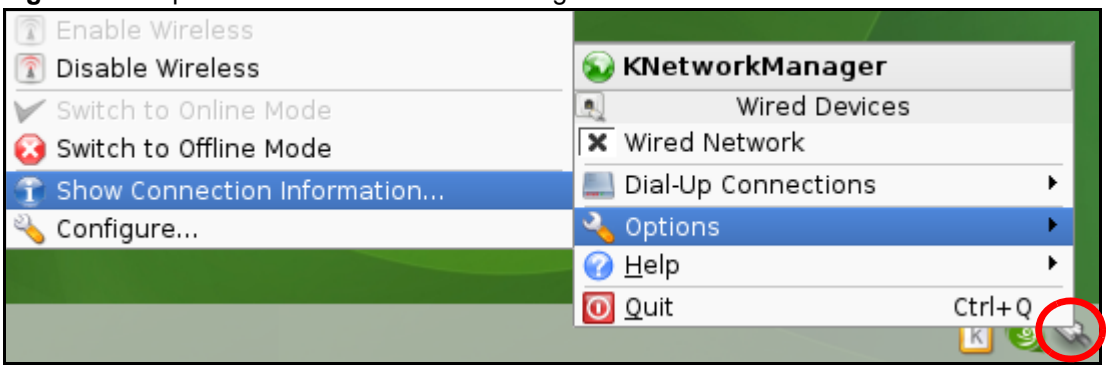


9 Click **Finish** to save your settings and close the window.

Verifying Settings

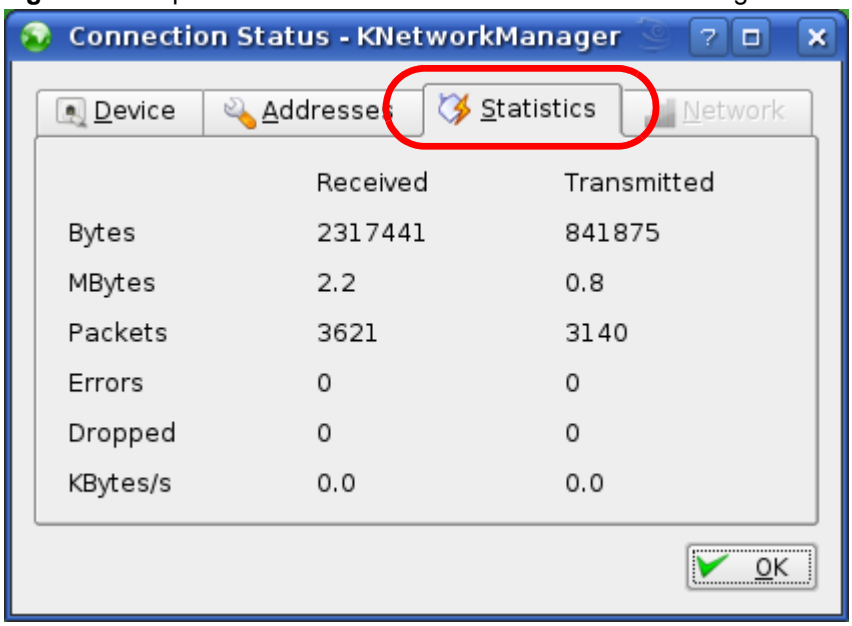
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 188 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 189 openSUSE: Connection Status - KNetwork Manager



B

Wireless LANs

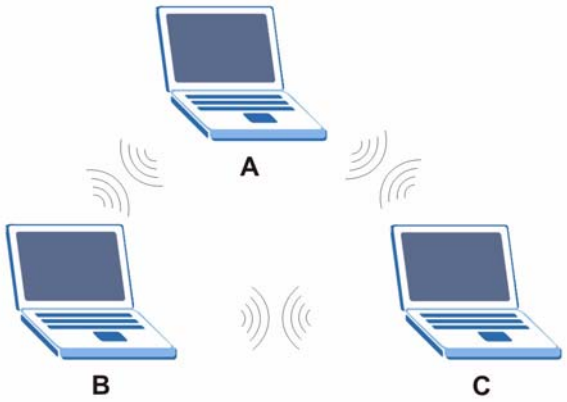
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 190 Peer-to-Peer Communication in an Ad-hoc Network

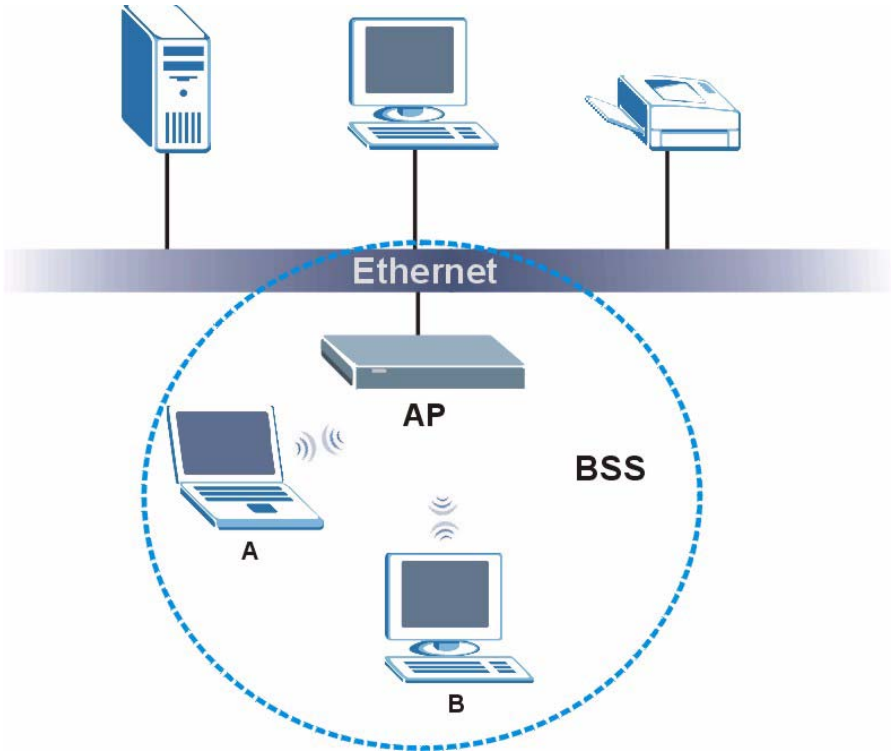


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 191 Basic Service Set



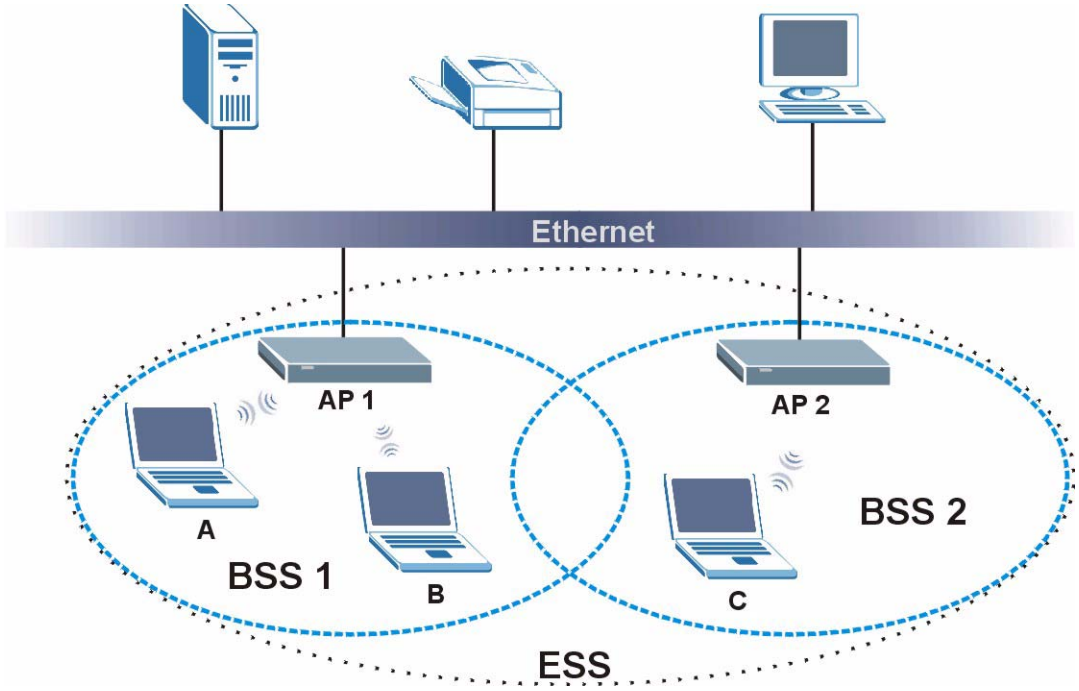
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 192 Infrastructure WLAN



Channel

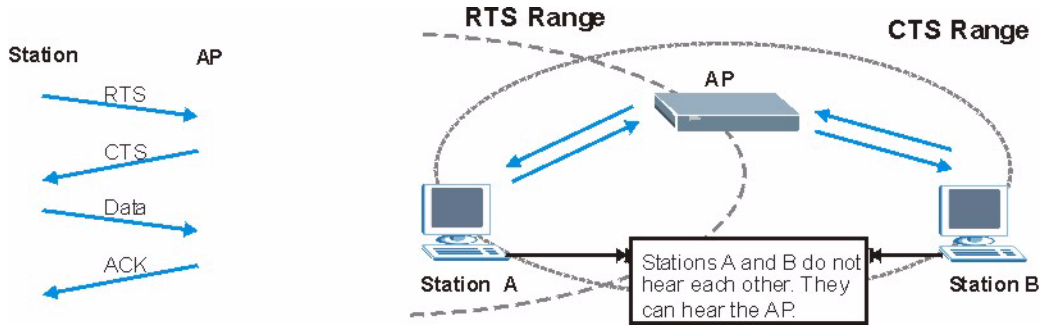
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 193 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. **Short** and **Long** refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support long preamble, but not all support short preamble.

Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.

Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.

Select **Dynamic** to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.

The AP and the wireless adapters MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 85 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 86 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
  Determines the identity of the users.
- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting
  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
  Sent by an access point requesting authentication.
- Access-Reject
  Sent by a RADIUS server rejecting access.
- Access-Accept
  Sent by a RADIUS server allowing access.
- Access-Challenge
  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
  Sent by the access point requesting accounting.
- Accounting-Response
  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 87 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

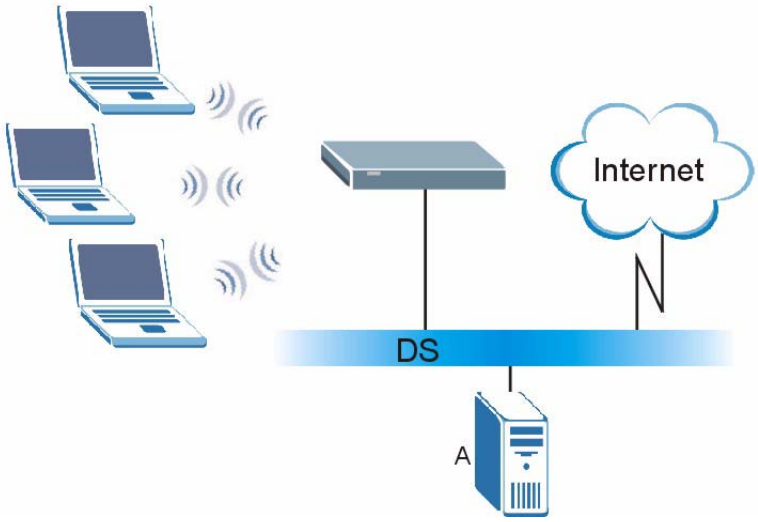
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 194 WPA(2) with RADIUS Application Example



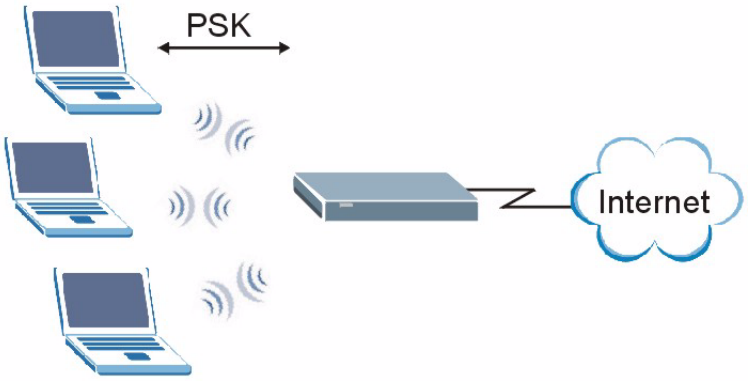
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP and wireless clients use the pre-shared key to generate a common PMK (Pairwise Master Key).

4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 195 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 88 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

C

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

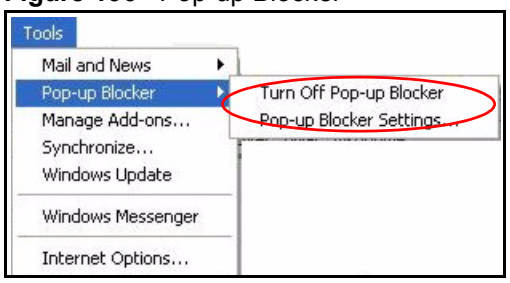
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 196 Pop-up Blocker

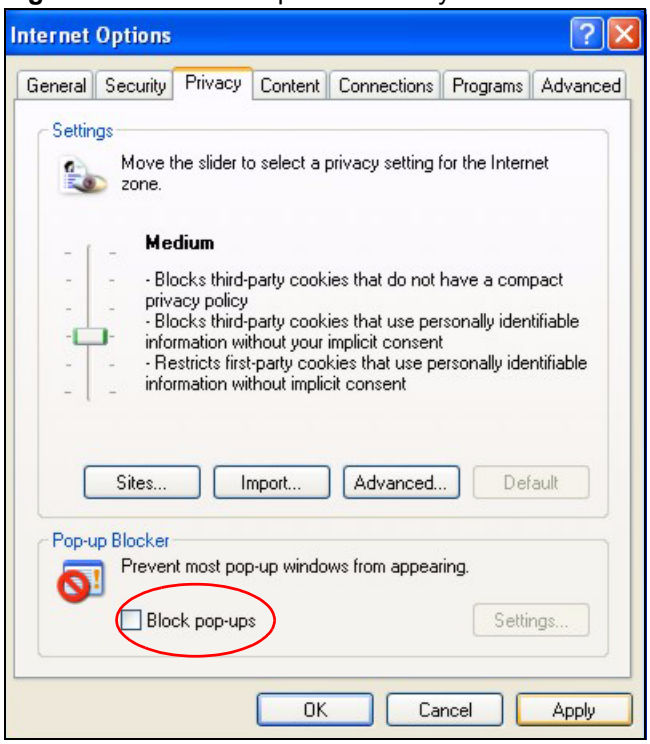


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 197 Internet Options: Privacy



3 Click **Apply** to save this setting.

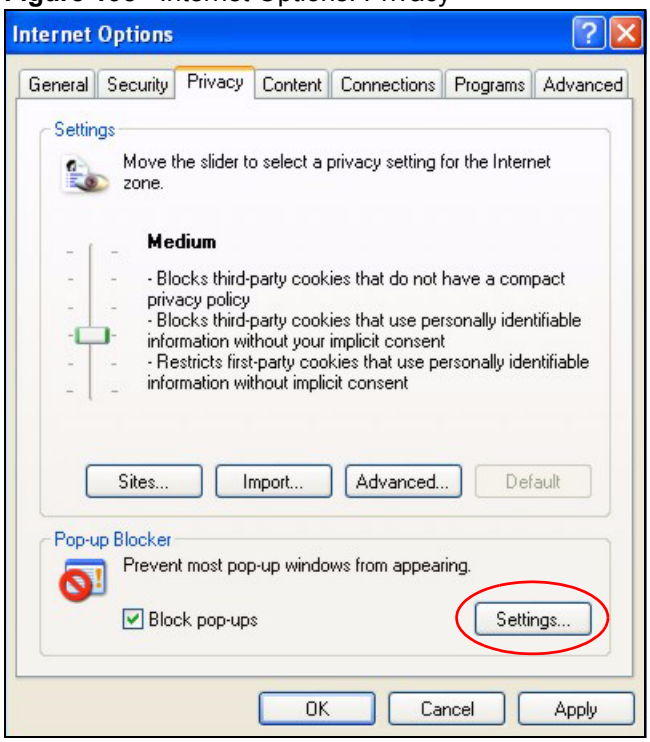
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

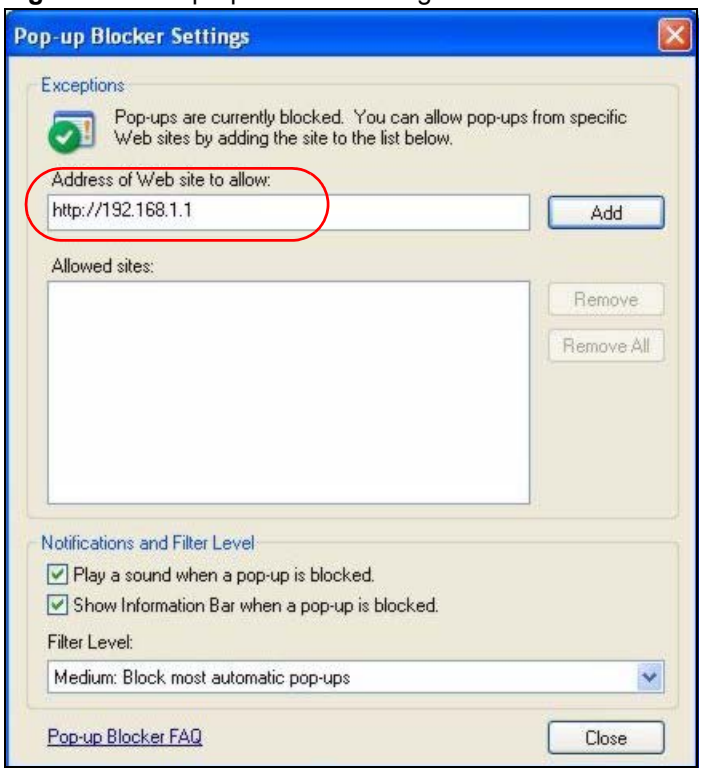
Figure 198 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 199 Pop-up Blocker Settings



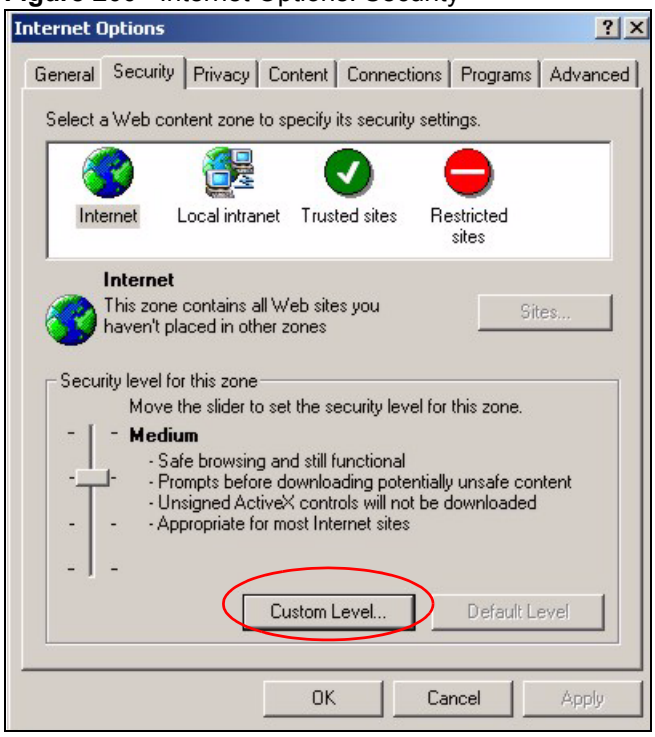
5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

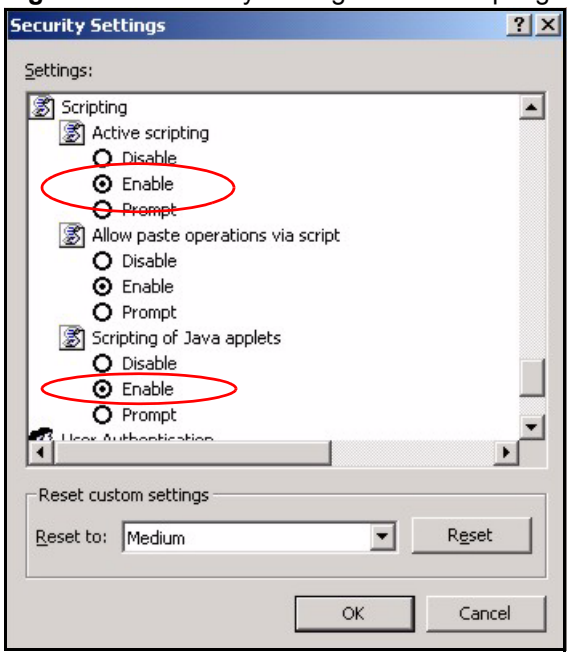
1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 200 Internet Options: Security



2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

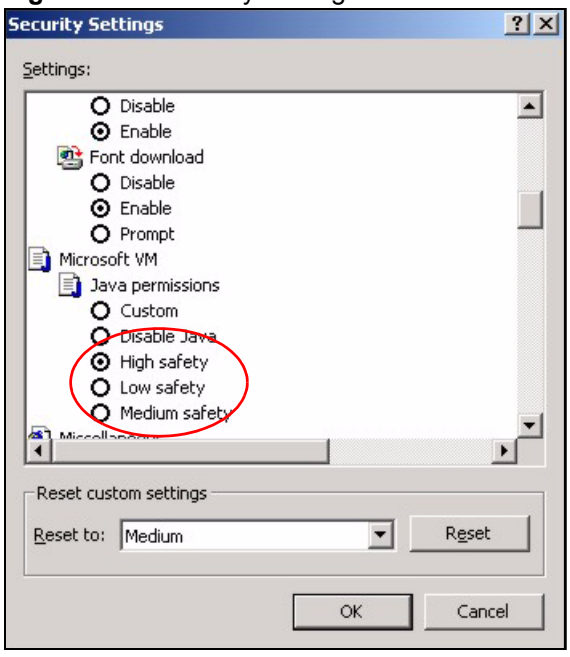
Figure 201 Security Settings - Java Scripting



Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

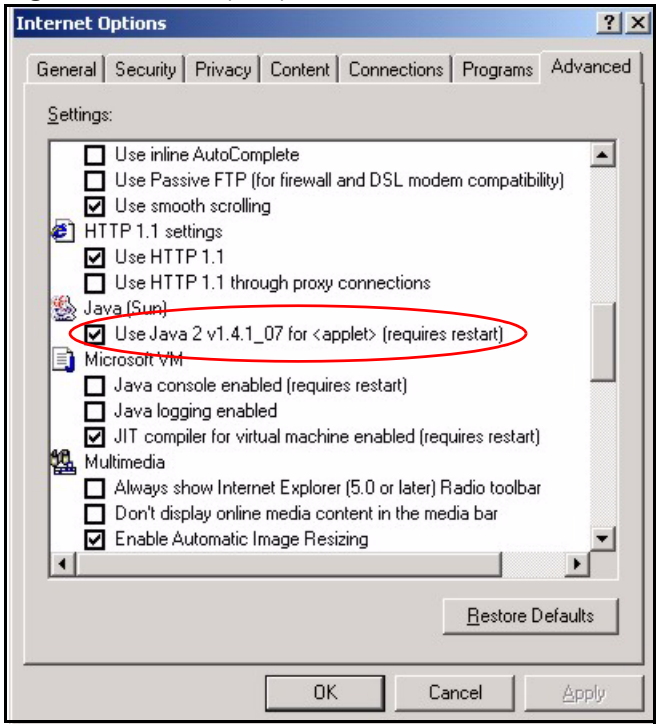
Figure 202 Security Settings - Java



JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3 Click **OK** to close the window.

Figure 203 Java (Sun)



D

Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon ( ) somewhere in the main browser window (not all browsers show the padlock in the same location.)

In this appendix, you can import a public key certificate for:

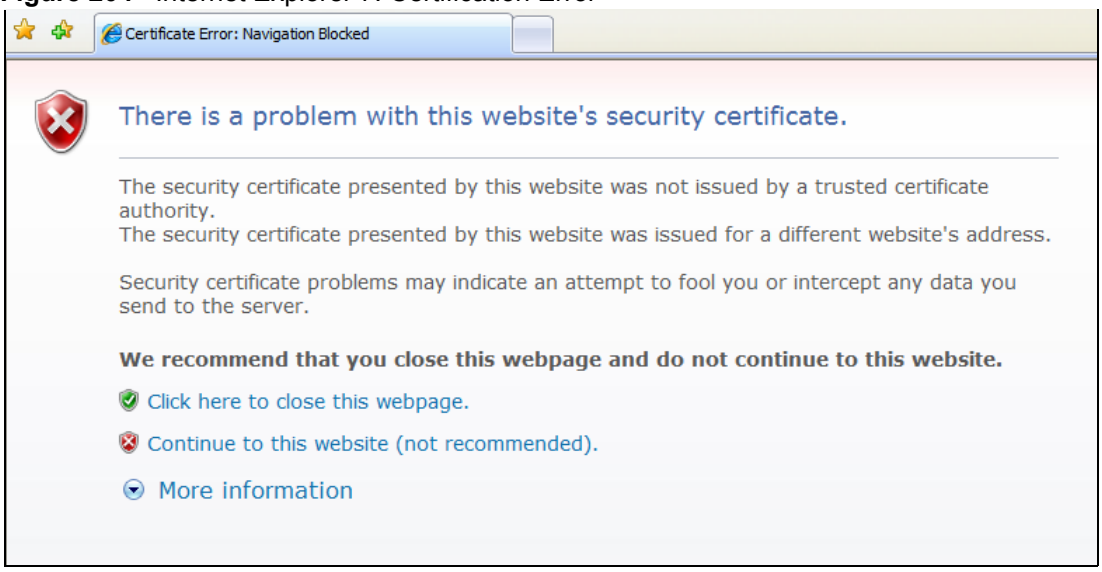
- Internet Explorer on page 289
- Firefox on page 297
- Opera on page 302
- Konqueror on page 308

Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

Figure 204 Internet Explorer 7: Certification Error

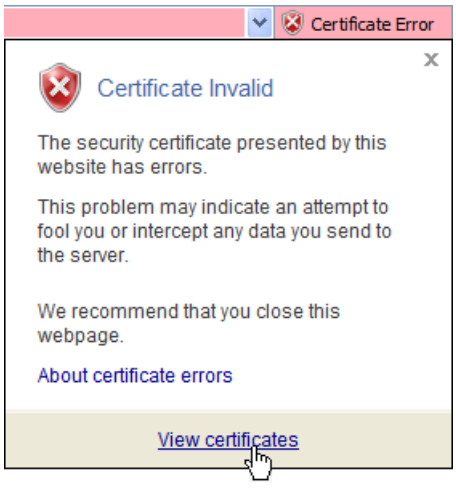


2 Click **Continue to this website (not recommended)**.

Figure 205 Internet Explorer 7: Certification Error

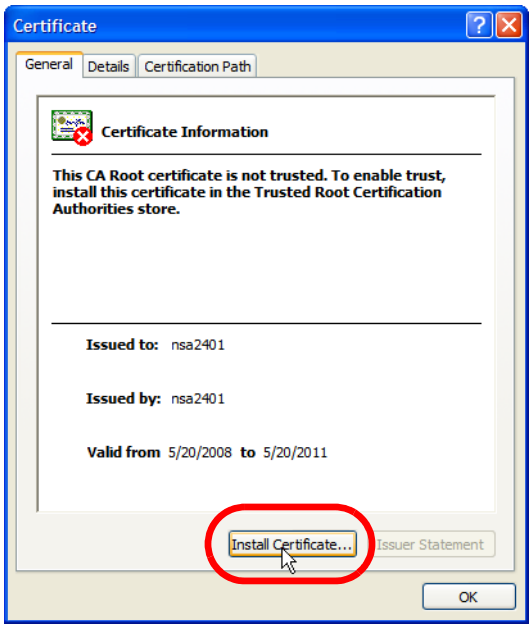
3 In the **Address Bar**, click **Certificate Error** > **View certificates**.

Figure 206 Internet Explorer 7: Certificate Error



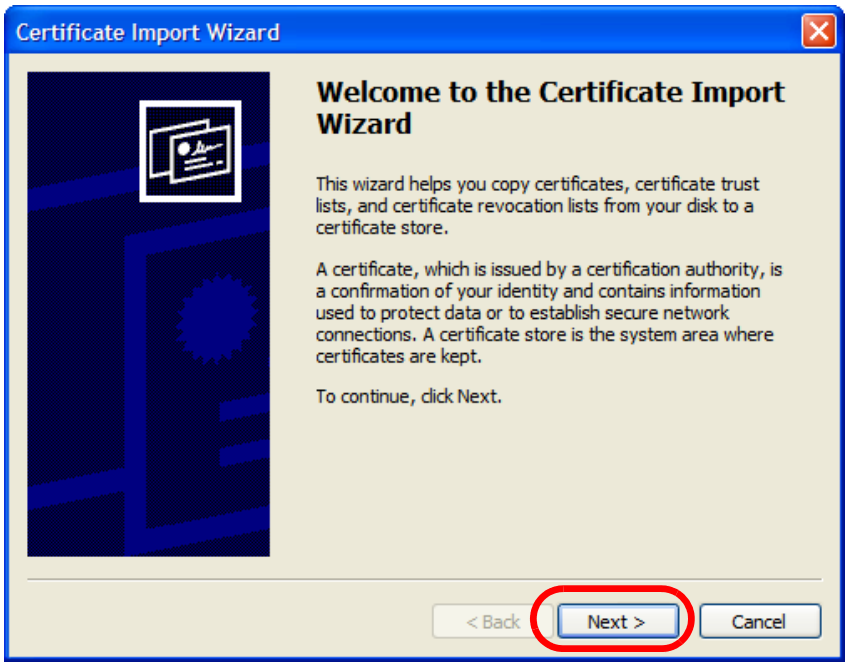
4 In the **Certificate** dialog box, click **Install Certificate**.

Figure 207 Internet Explorer 7: Certificate



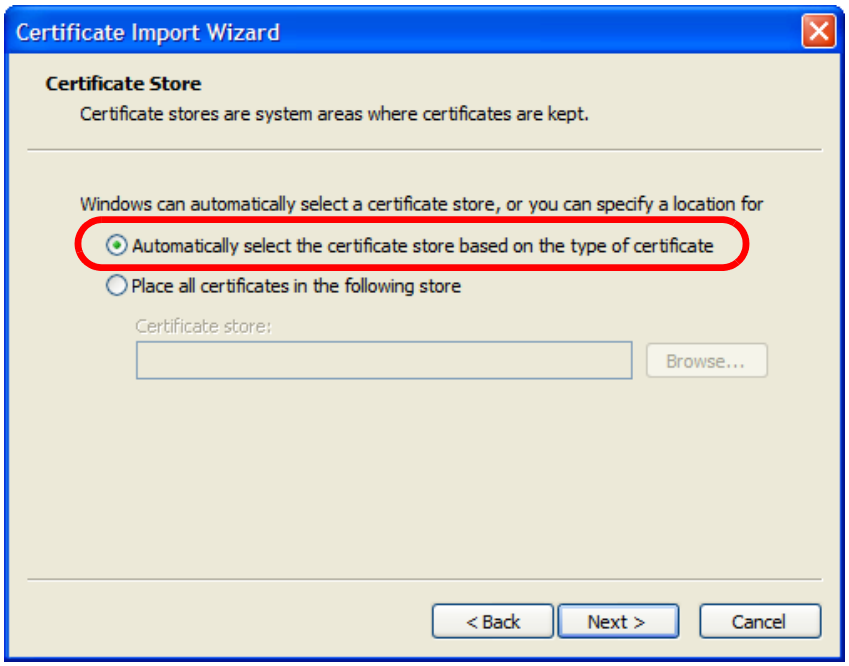
5 In the **Certificate Import Wizard**, click **Next**.

Figure 208 Internet Explorer 7: Certificate Import Wizard



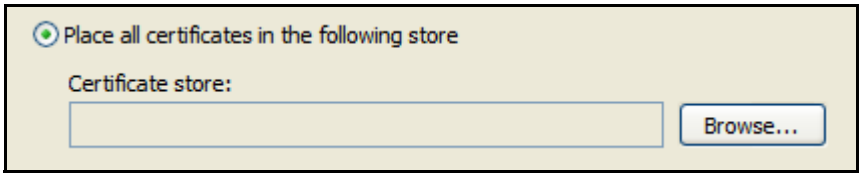
6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

Figure 209 Internet Explorer 7: Certificate Import Wizard



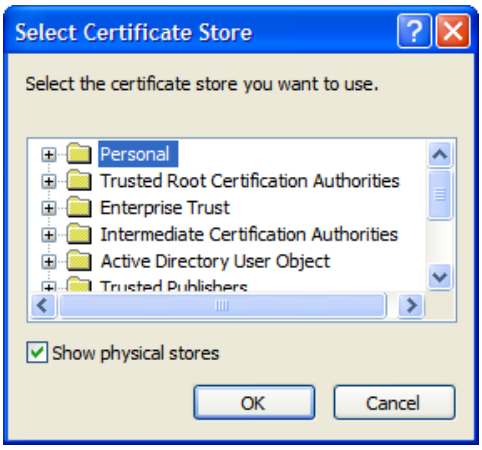
7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

Figure 210 Internet Explorer 7: Certificate Import Wizard



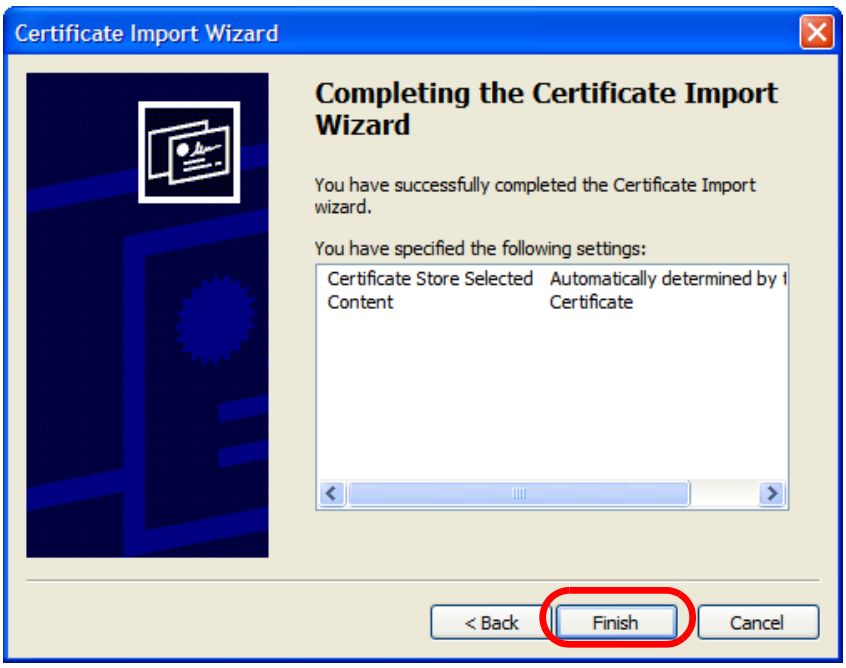
8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

Figure 211 Internet Explorer 7: Select Certificate Store



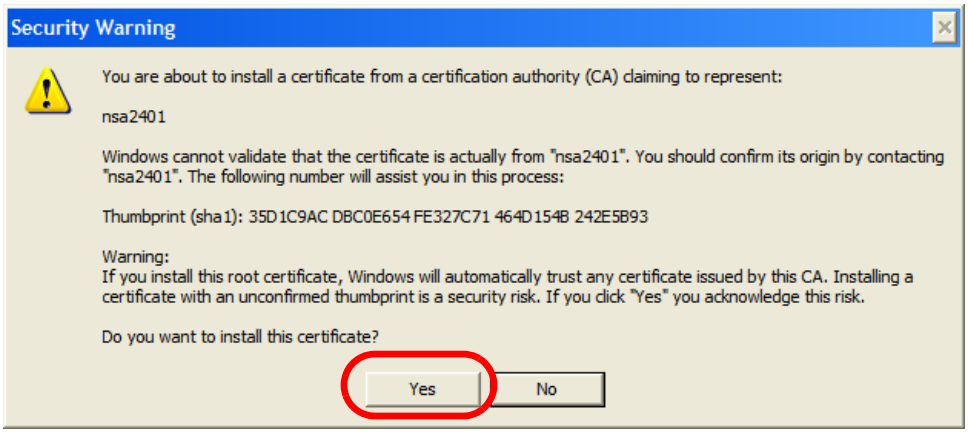
9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

Figure 212 Internet Explorer 7: Certificate Import Wizard



10 If you are presented with another **Security Warning**, click **Yes**.

Figure 213 Internet Explorer 7: Security Warning

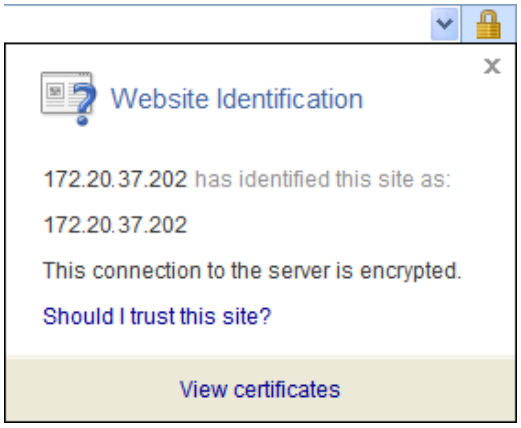


11 Finally, click **OK** when presented with the successful certificate installation message.

Figure 214 Internet Explorer 7: Certificate Import Wizard

12 The next time you start Internet Explorer and go to a ZyXEL web configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

Figure 215 Internet Explorer 7: Website Identification



Installing a Stand-Alone Certificate File in Internet Explorer

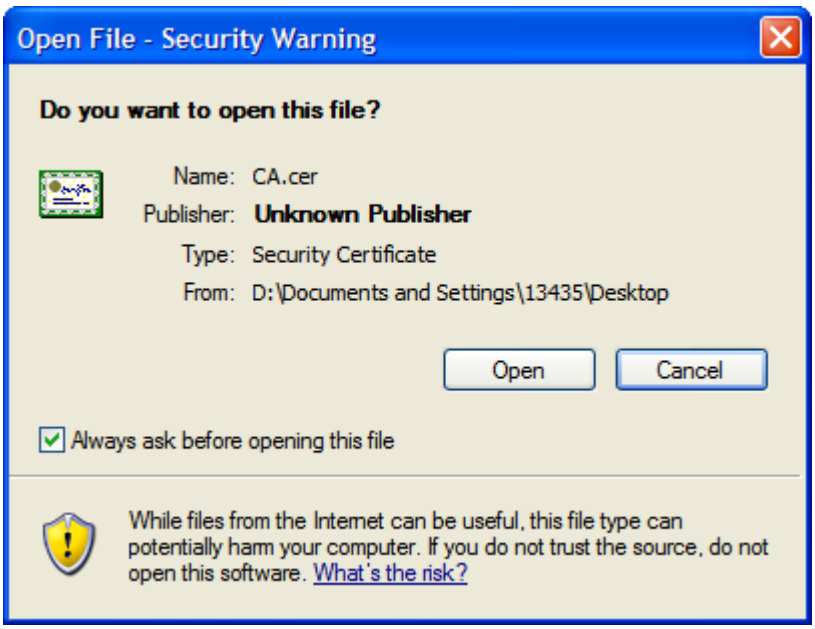
Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 216 Internet Explorer 7: Public Key Certificate File

2 In the security warning dialog box, click **Open**.

Figure 217 Internet Explorer 7: Open File - Security Warning



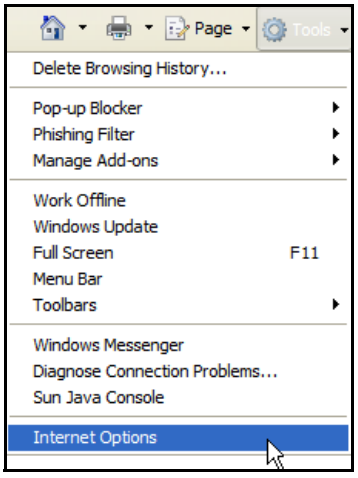
3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 289 to complete the installation process.

Removing a Certificate in Internet Explorer

This section shows you how to remove a public key certificate in Internet Explorer 7.

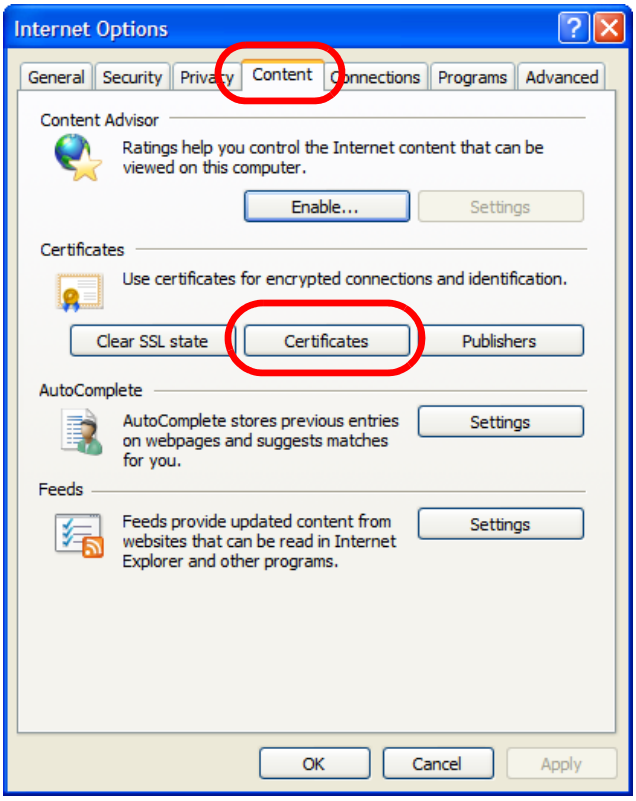
1 Open **Internet Explorer** and click **Tools > Internet Options**.

Figure 218 Internet Explorer 7: Tools Menu



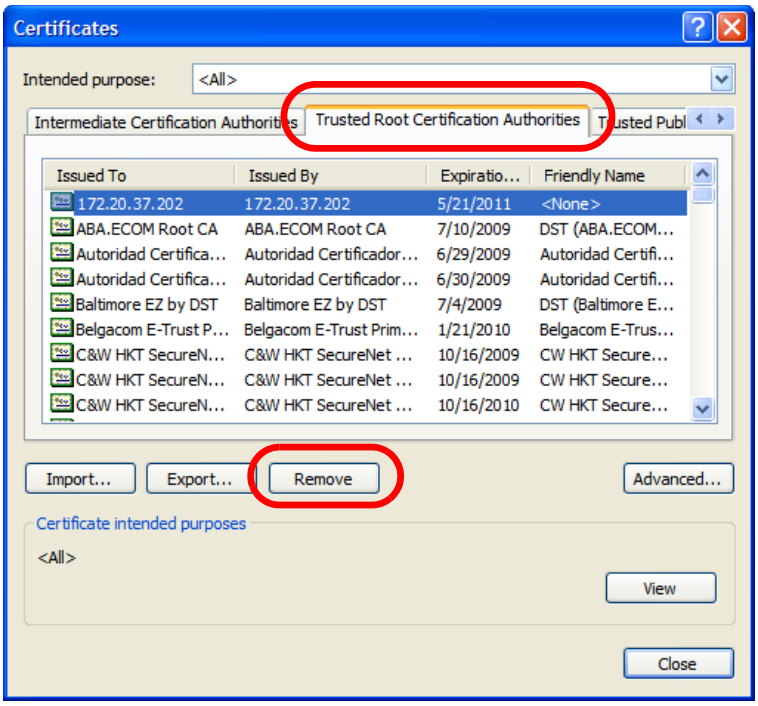
2 In the **Internet Options** dialog box, click **Content** > **Certificates**.

Figure 219 Internet Explorer 7: Internet Options



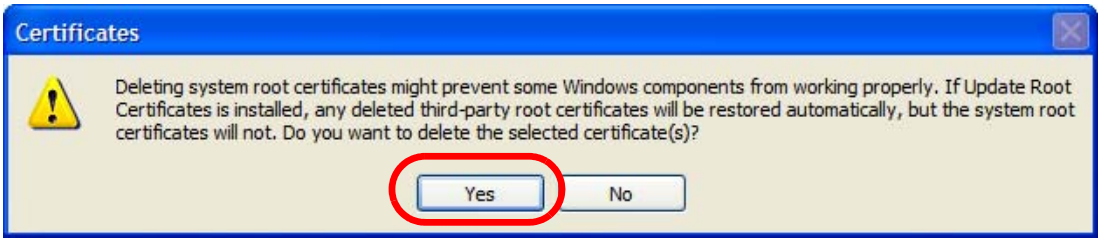
3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

Figure 220 Internet Explorer 7: Certificates



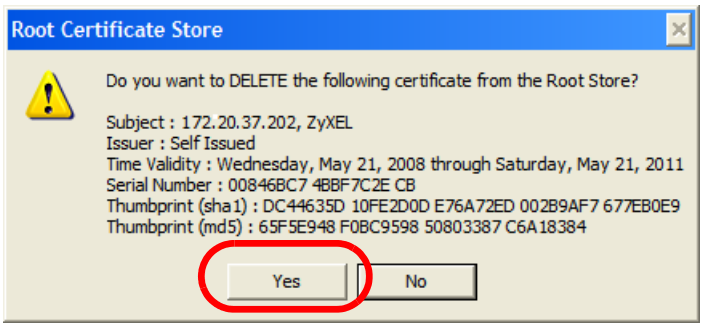
4 In the **Certificates** confirmation, click **Yes**.

Figure 221 Internet Explorer 7: Certificates



5 In the **Root Certificate Store** dialog box, click **Yes**.

Figure 222 Internet Explorer 7: Root Certificate Store



6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

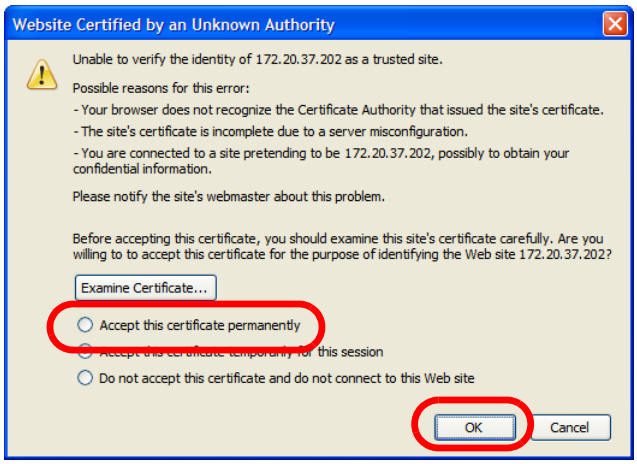
Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

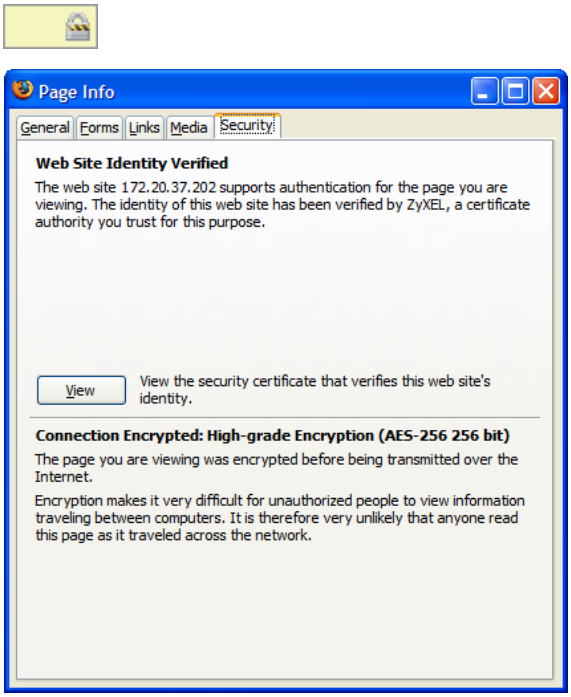
2 Select **Accept this certificate permanently** and click **OK.**

Figure 223 Firefox 2: Website Certified by an Unknown Authority



3 The certificate is stored and you can now connect securely to the web configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info** > **Security** window to view the web page's security information.

Figure 224 Firefox 2: Page Info

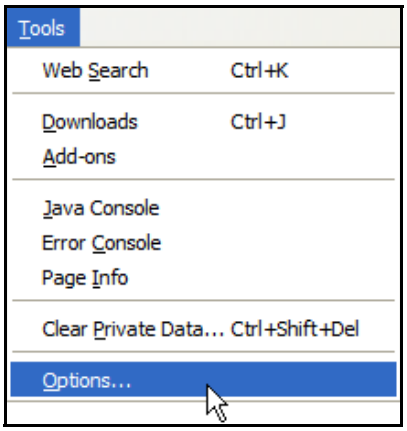


Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

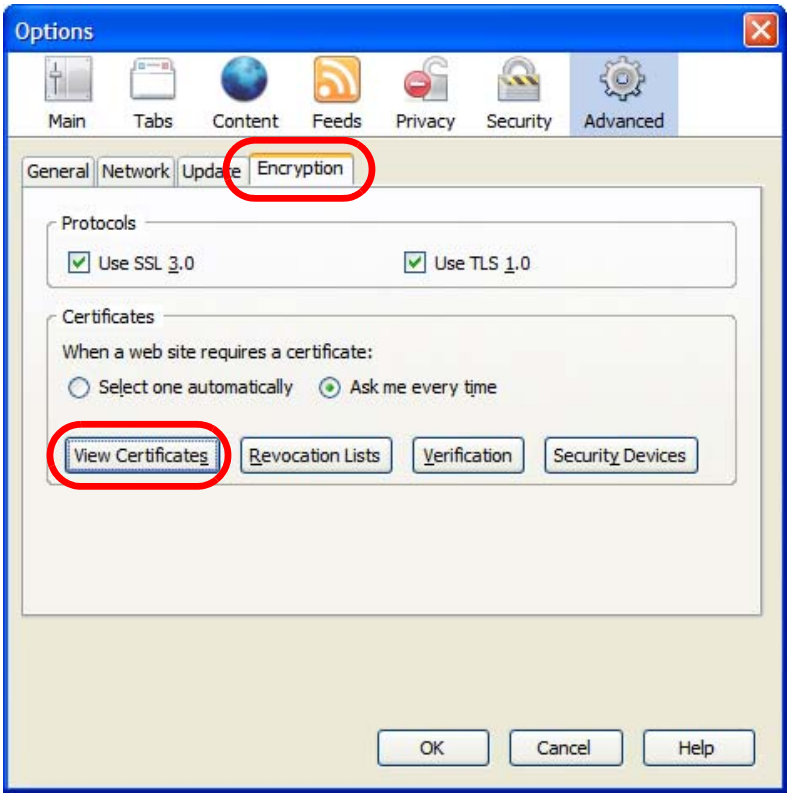
1 Open **Firefox** and click **Tools** > **Options**.

Figure 225 Firefox 2: Tools Menu



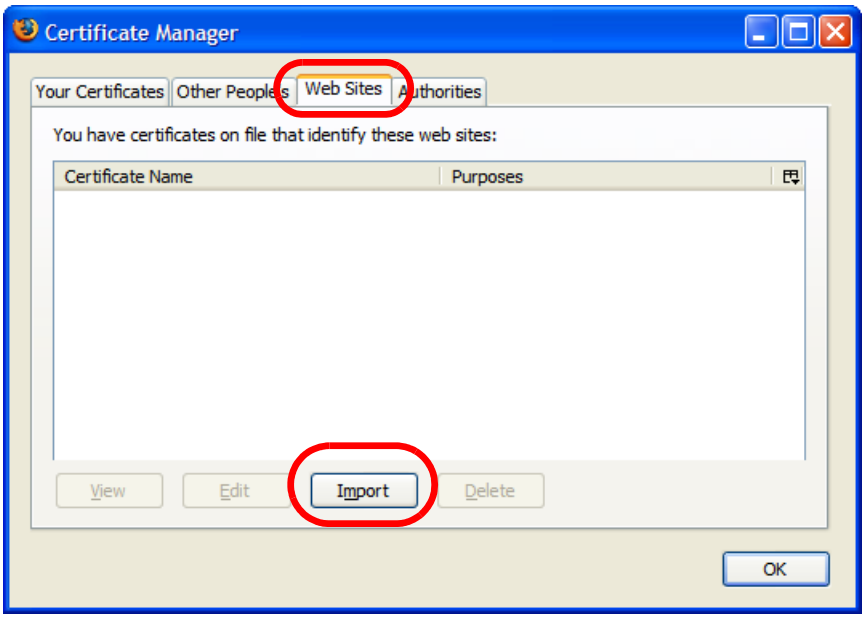
2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

Figure 226 Firefox 2: Options



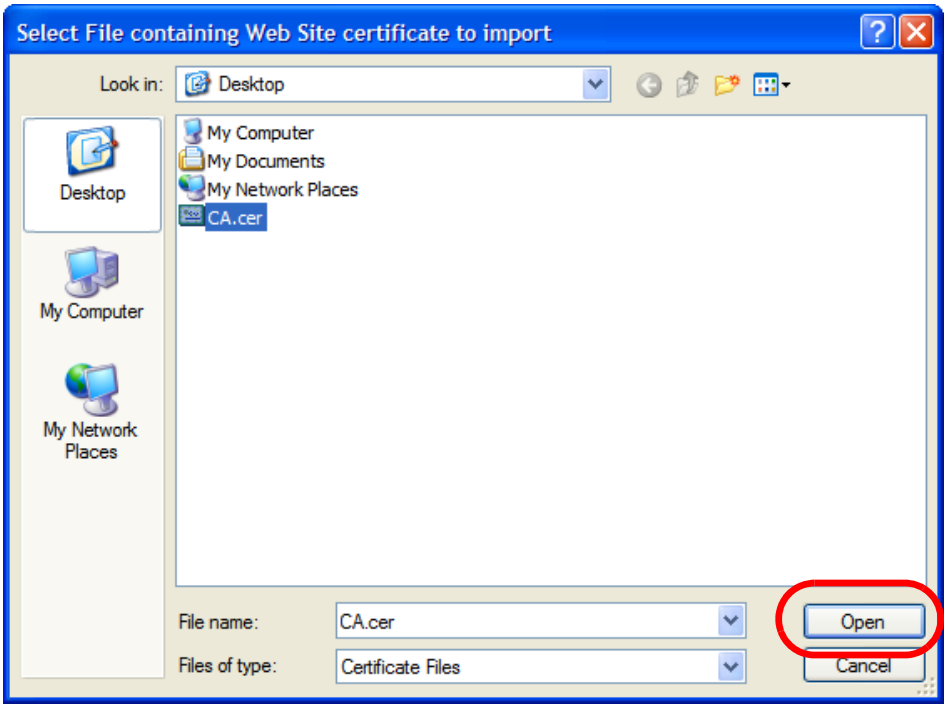
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

Figure 227 Firefox 2: Certificate Manager



4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

Figure 228 Firefox 2: Select File



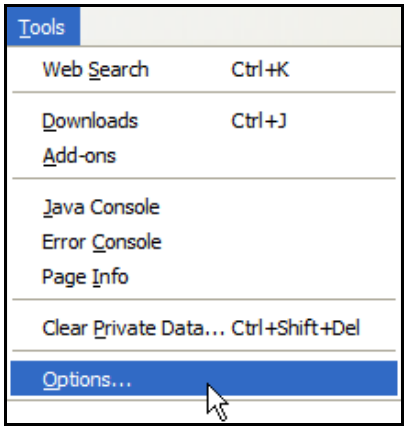
5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

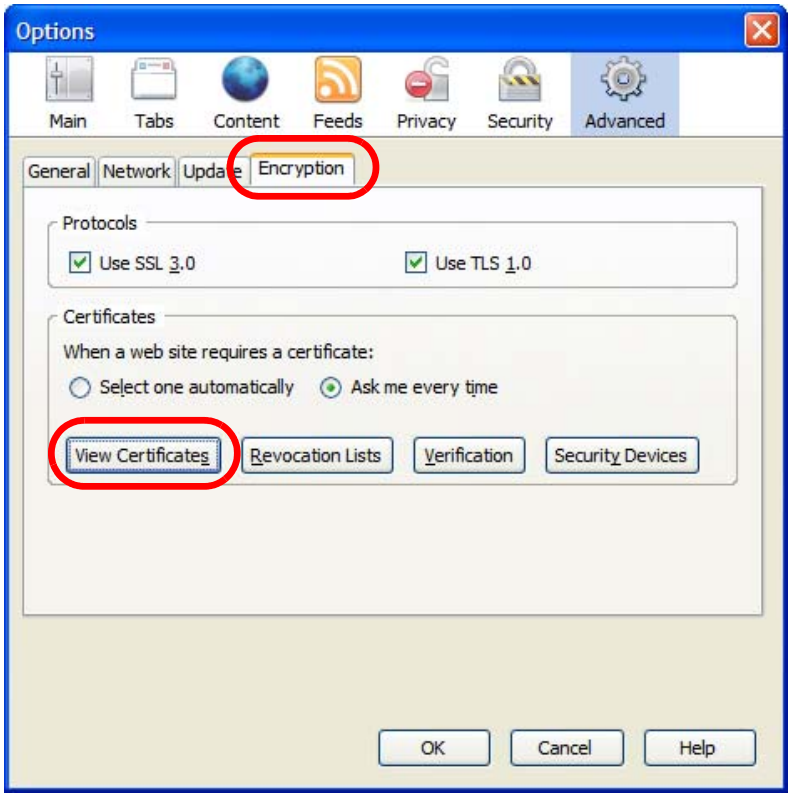
1 Open **Firefox** and click **Tools** > **Options**.

Figure 229 Firefox 2: Tools Menu



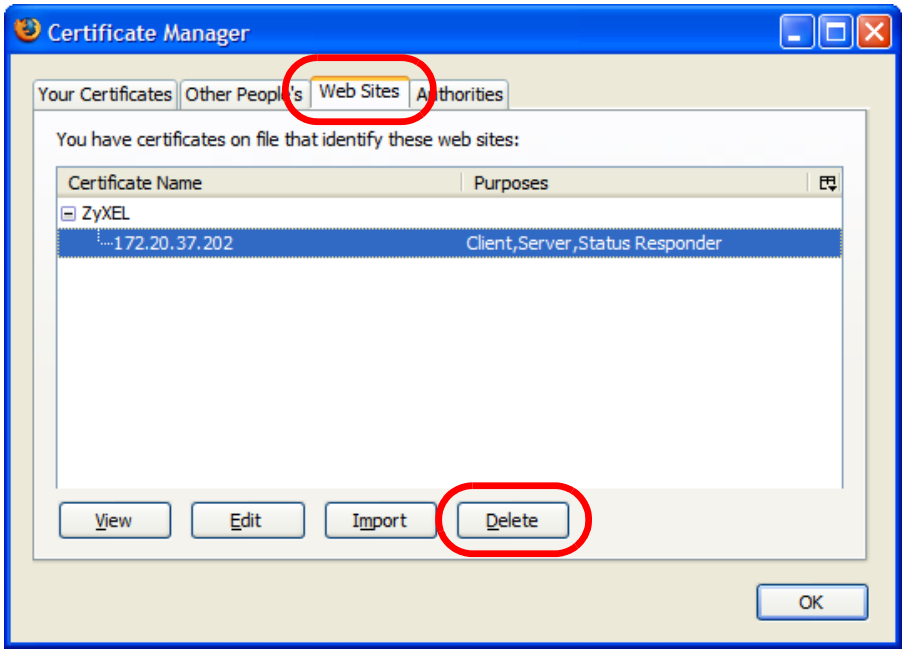
2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

Figure 230 Firefox 2: Options



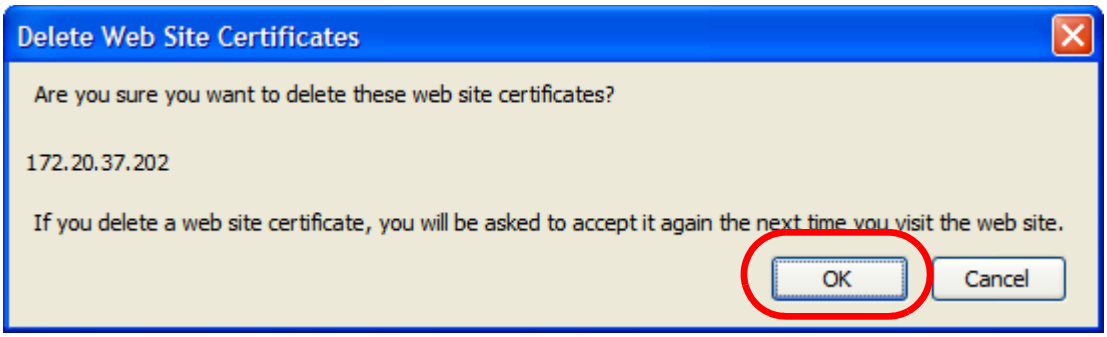
3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 231 Firefox 2: Certificate Manager



4 In the **Delete Web Site Certificates** dialog box, click **OK**.

Figure 232 Firefox 2: Delete Web Site Certificates



5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

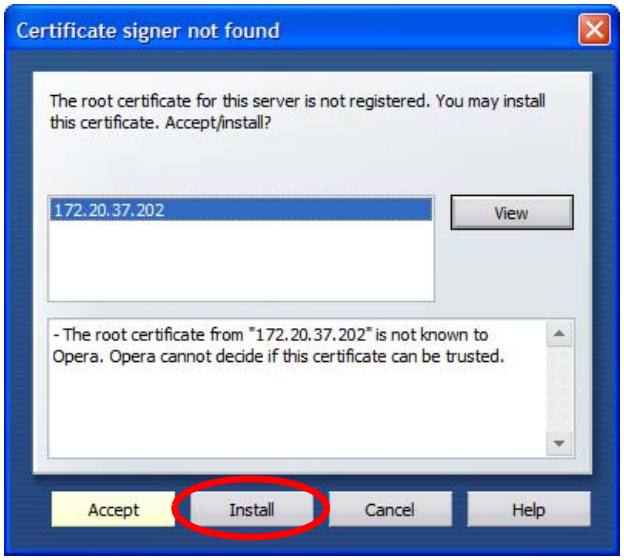
Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

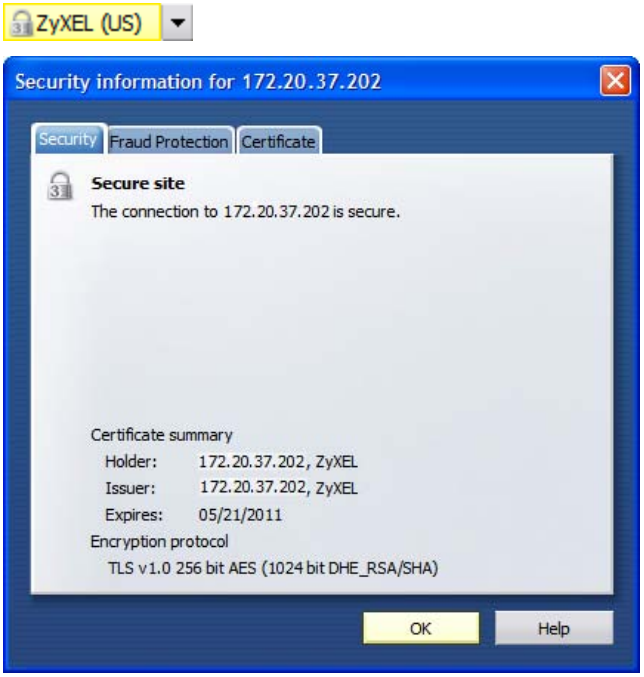
2 Click **Install** to accept the certificate.

Figure 233 Opera 9: Certificate signer not found



3 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Figure 234 Opera 9: Security information

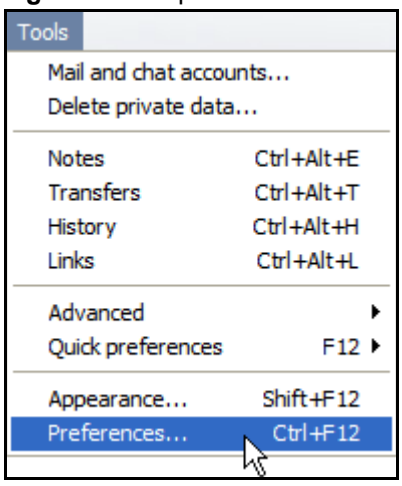


Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

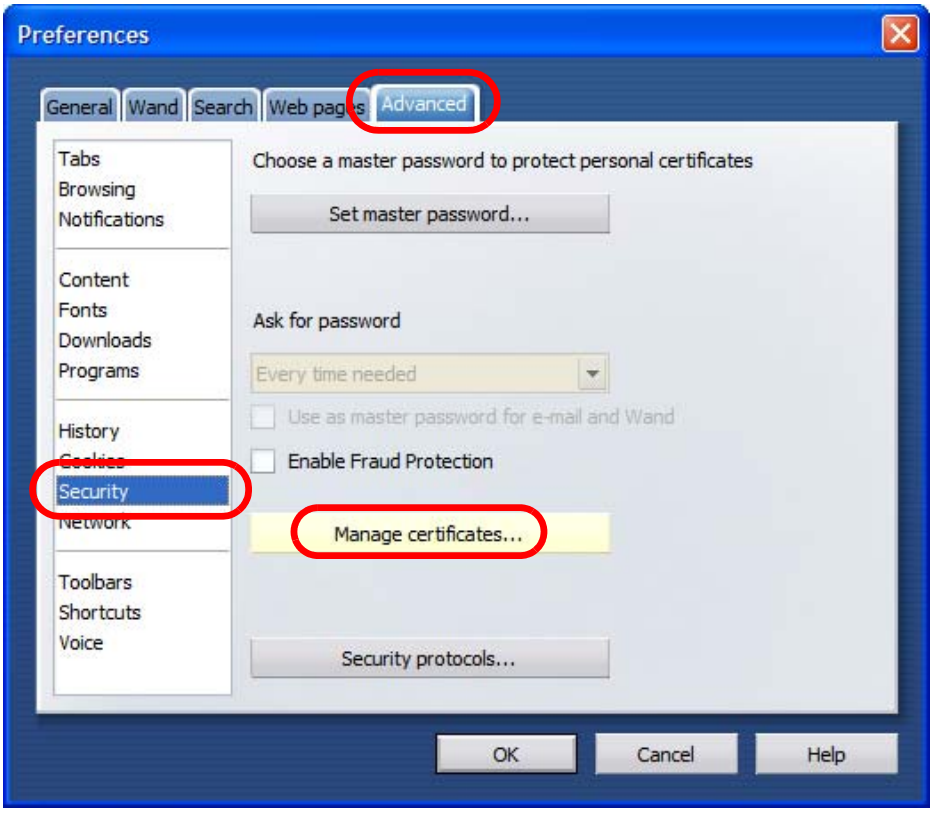
1 Open **Opera** and click **Tools** > **Preferences**.

Figure 235 Opera 9: Tools Menu



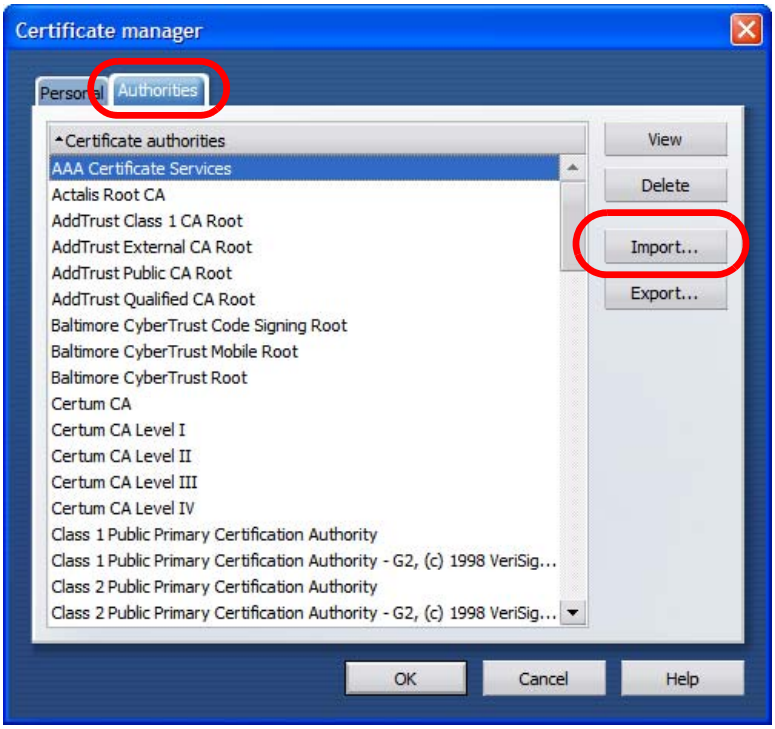
2 In **Preferences**, click **Advanced** > **Security** > **Manage certificates**.

Figure 236 Opera 9: Preferences



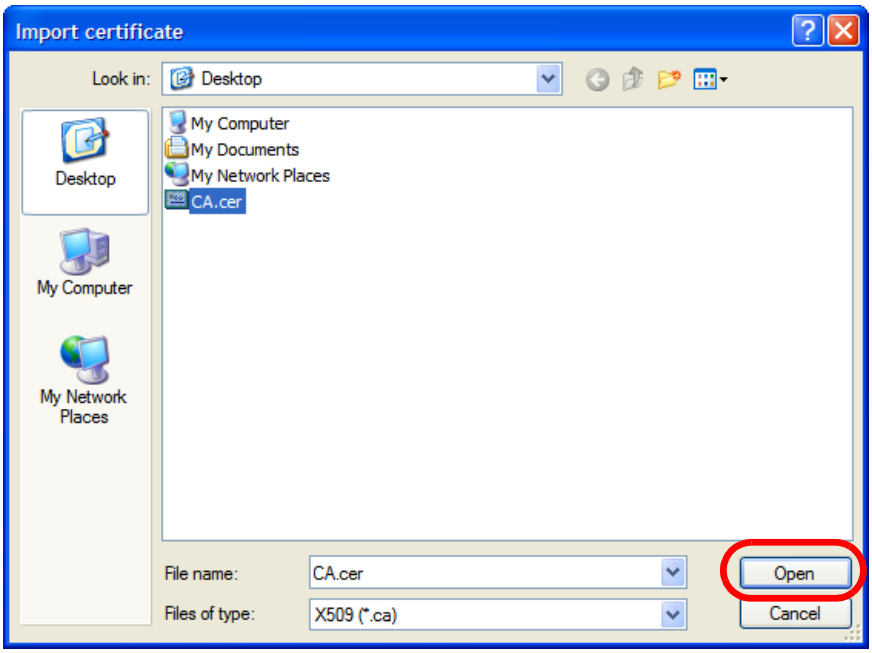
3 In the **Certificates Manager**, click **Authorities** > **Import**.

Figure 237 Opera 9: Certificate manager



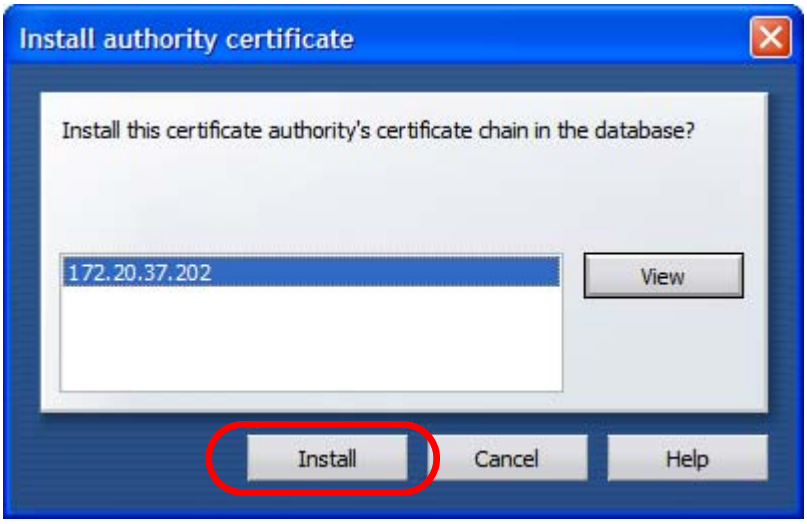
4 Use the **Import certificate** dialog box to locate the certificate and then click **Open.**

Figure 238 Opera 9: Import certificate



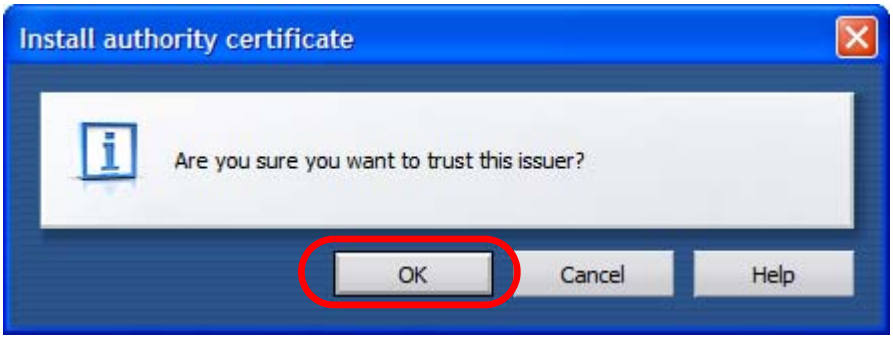
5 In the **Install authority certificate** dialog box, click **Install**.

Figure 239 Opera 9: Install authority certificate



6 Next, click **OK**.

Figure 240 Opera 9: Install authority certificate



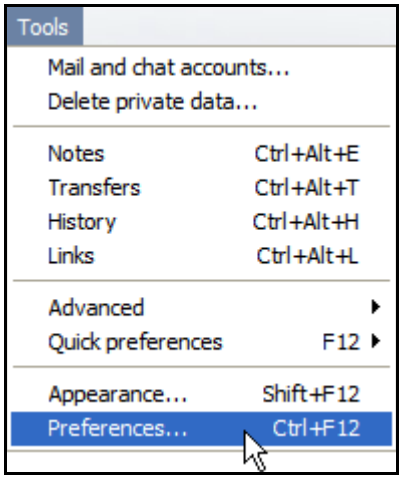
7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

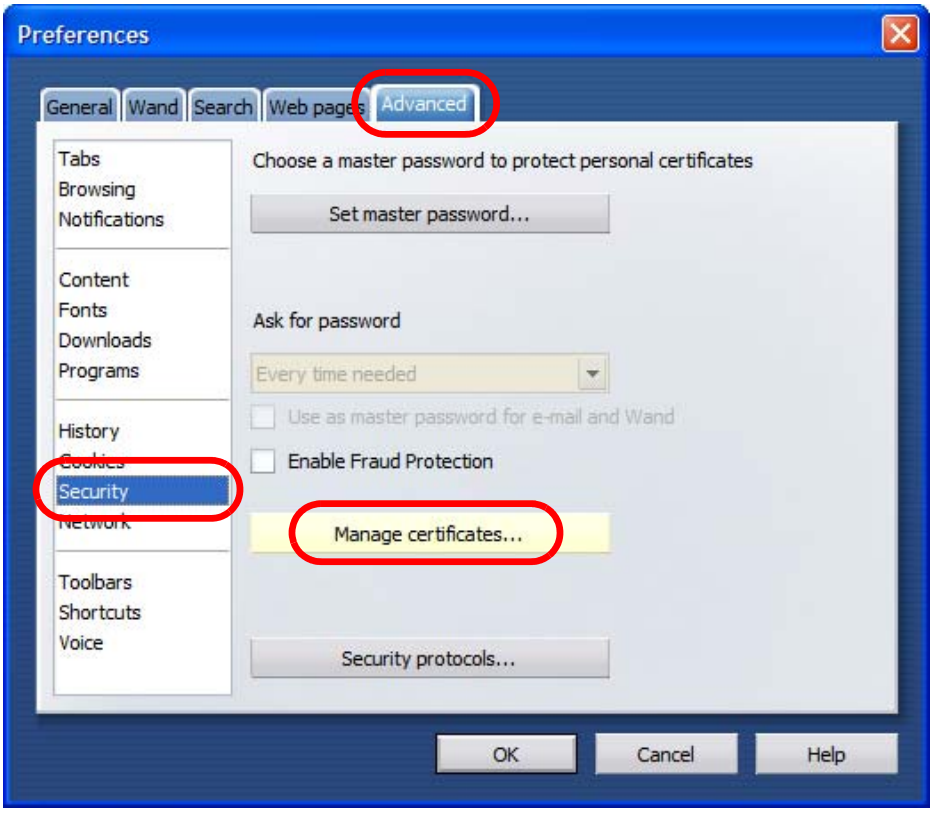
1 Open **Opera** and click **Tools** > **Preferences**.

Figure 241 Opera 9: Tools Menu



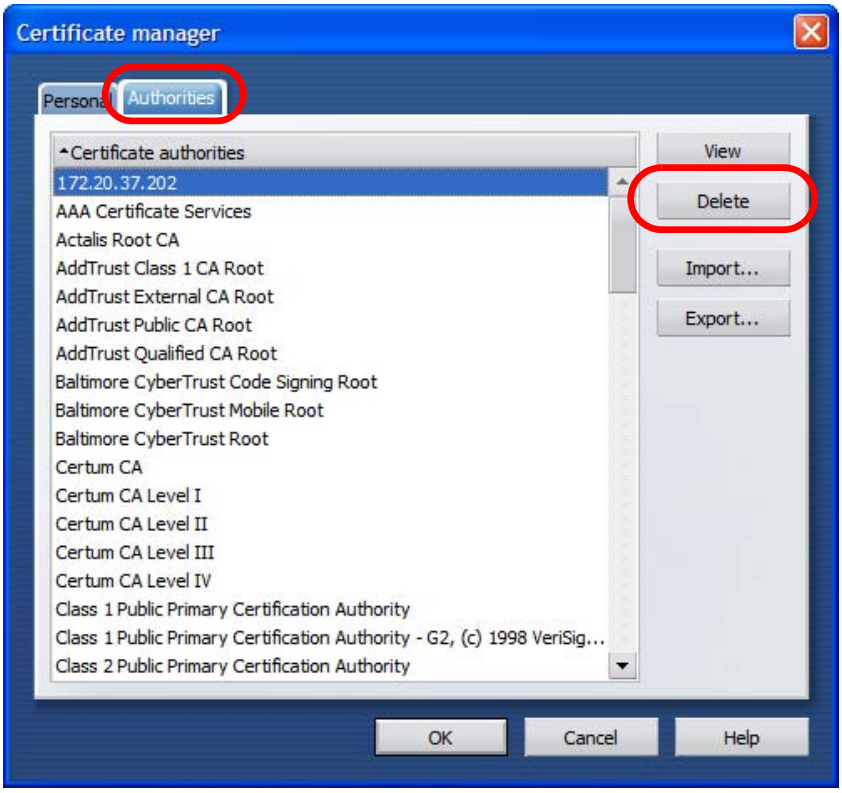
2 In **Preferences**, **Advanced** > **Security** > **Manage certificates**.

Figure 242 Opera 9: Preferences



3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 243 Opera 9: Certificate manager



4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

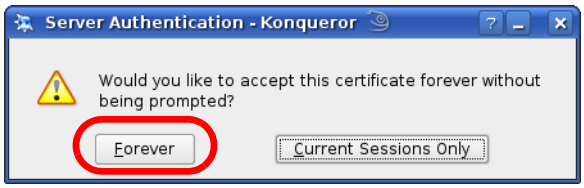
1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

2 Click **Continue**.

Figure 244 Konqueror 3.5: Server Authentication

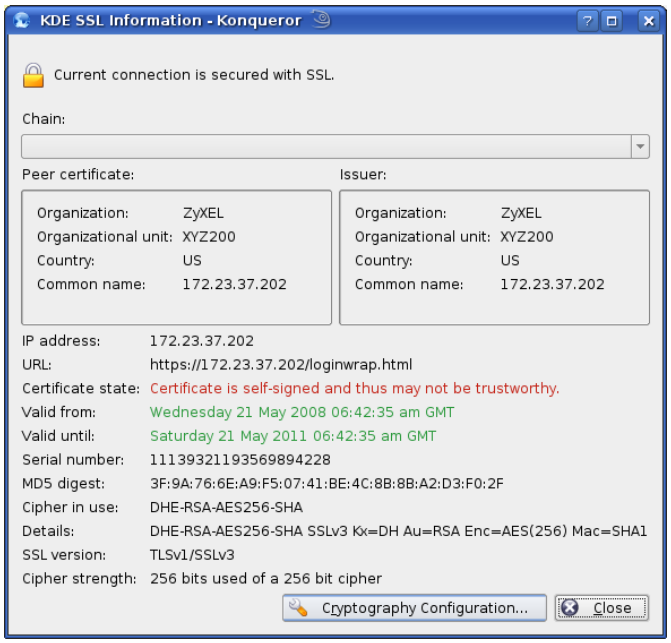
3 Click **Forever** when prompted to accept the certificate.

Figure 245 Konqueror 3.5: Server Authentication



4 Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

Figure 246 Konqueror 3.5: KDE SSL Information



Installing a Stand-Alone Certificate File in Konqueror

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

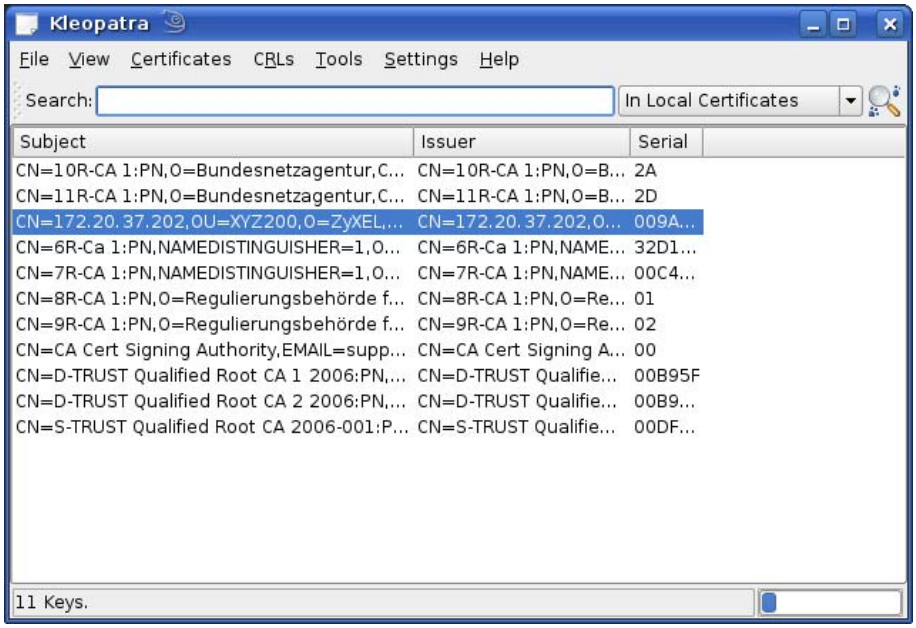
Figure 247 Konqueror 3.5: Public Key Certificate File

2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

Figure 248 Konqueror 3.5: Certificate Import Result

The public key certificate appears in the KDE certificate manager, **Kleopatra**.

Figure 249 Konqueror 3.5: Kleopatra



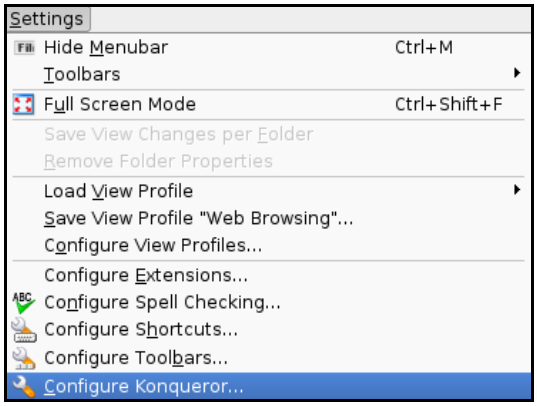
3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

1 Open **Konqueror** and click **Settings > Configure Konqueror**.

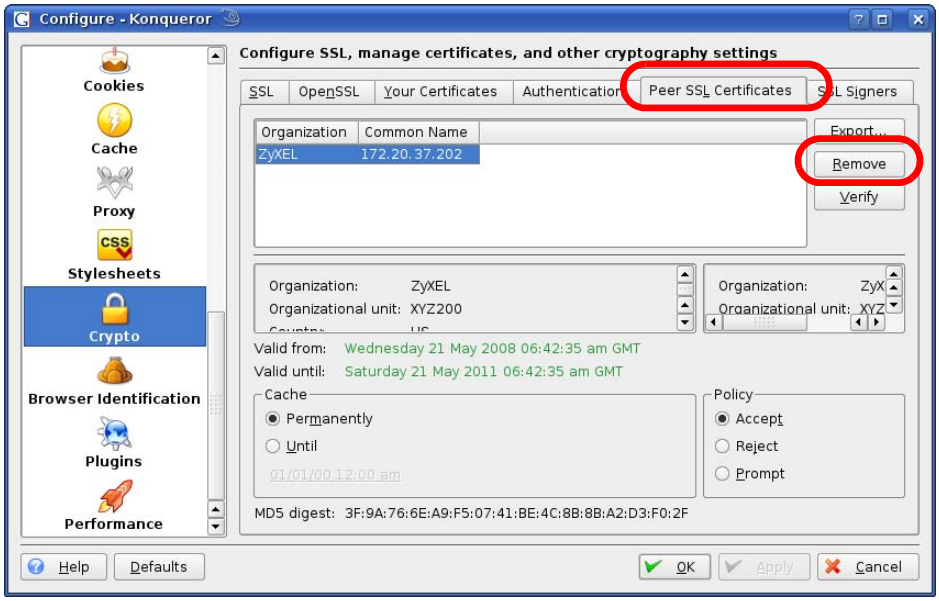
Figure 250 Konqueror 3.5: Settings Menu



2 In the **Configure** dialog box, select **Crypto**.

3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

Figure 251 Konqueror 3.5: Configure



4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.

E

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

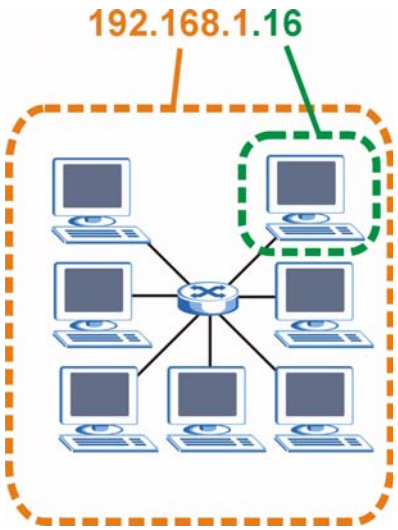
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 252 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 89 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 90 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 91 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 92 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 92 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

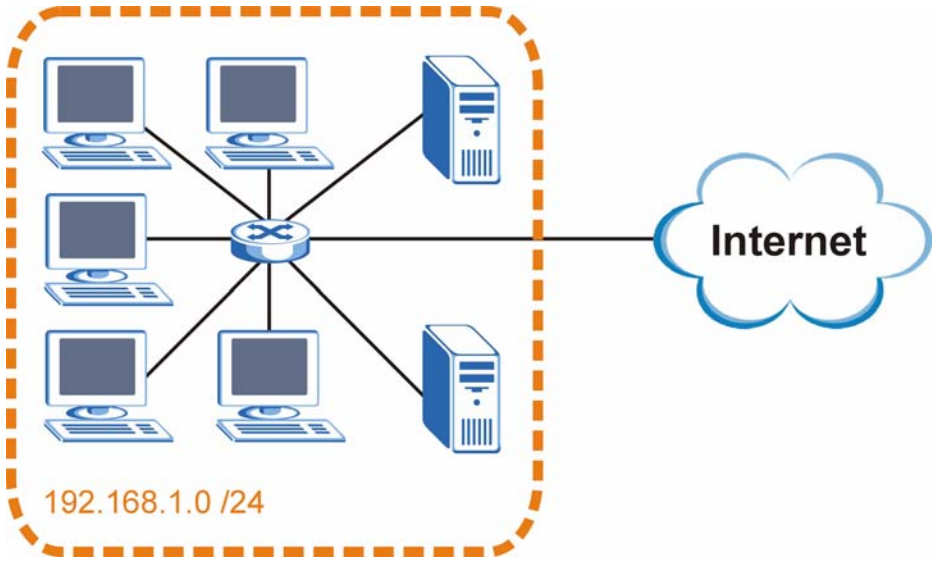
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 253 Subnetting Example: Before Subnetting

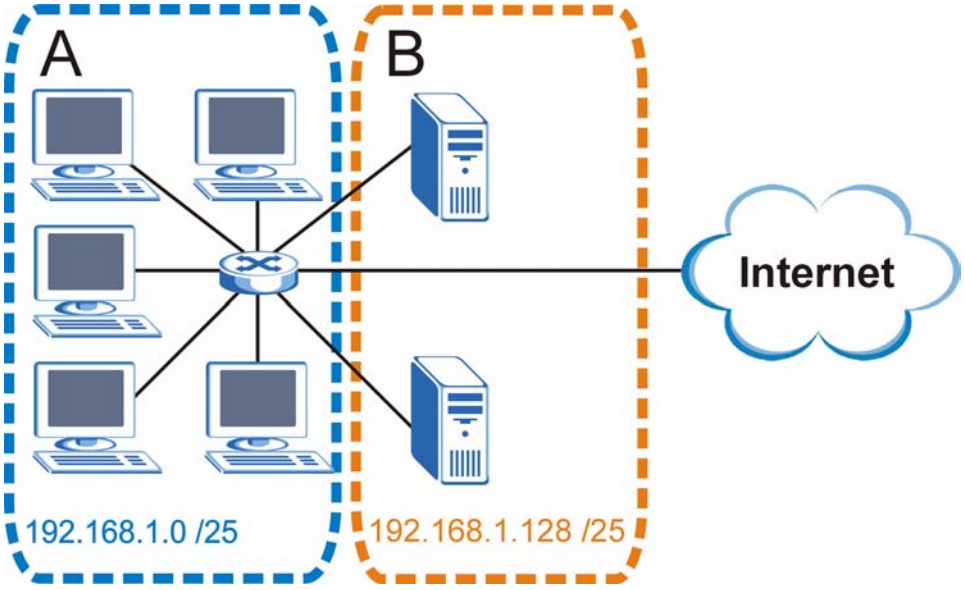


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 254 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 93 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 94 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 95 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 96 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 97 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 97 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 98 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 99 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 99 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

F

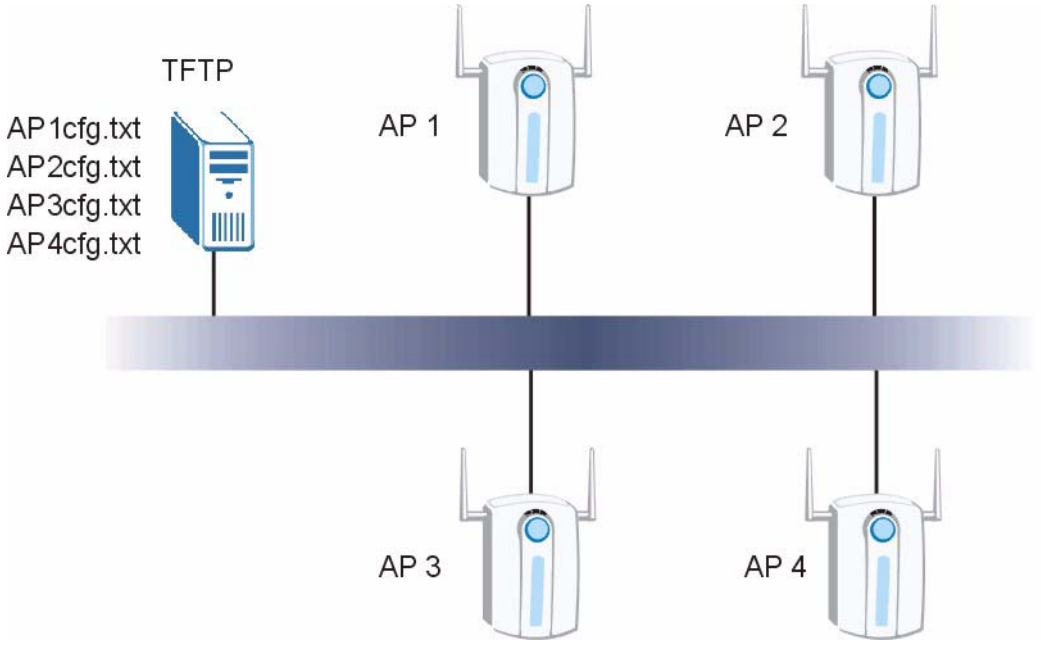
Text File Based Auto Configuration

This chapter describes how administrators can use text configuration files to configure the wireless LAN settings for multiple APs.

Text File Based Auto Configuration Overview

You can use plain text configuration files to configure the wireless LAN settings on multiple APs. The AP can automatically get a configuration file from a TFTP server at startup or after renewing DHCP client information.

Figure 255 Text File Based Auto Configuration



Use one of the following methods to give the AP the IP address of the TFTP server where you store the configuration files and the name of the configuration file that it should download.

You can have a different configuration file for each AP. You can also have multiple APs use the same configuration file.

If adjacent APs use the same configuration file, you should leave out the channel setting since they could interfere with each other's wireless traffic.

Auto Configuration by DHCP

A DHCP response can use options 66 and 67 to assign a TFTP server IP address and a filename. If the AP is configured as a DHCP client, these settings can be used to perform auto configuration.

Table 100 Auto Configuration by DHCP

COMMAND	DESCRIPTION
`wcfg autocfg dhcp [enable | disable]`	Turn configuration of TFTP server IP address and filename through DHCP on or off.

If this feature is enabled and the DHCP response provides a TFTP server IP address and a filename, the AP will try to download the file from the specified TFTP server. The AP then uses the file to configure wireless LAN settings.

Not all DHCP servers allow you to specify options 66 and 67.

Manual Configuration

Use the following command to manually configure a TFTP server IP address and a file name for the AP to use for auto provisioning whenever the AP starts up. See Section 25.1 on page 257 for how to access the Command Interpreter (CI).

Table 101 Manual Configuration

COMMAND	DESCRIPTION
`wcfg autocfg server [IP] [filename]`	Specify the TFTP server IP address and file name from which the AP is to download a configuration file whenever the AP starts up.

Configuration Via SNMP

You can configure and trigger the auto configuration remotely via SNMP.

Use the following procedure to have the AP download the configuration file.

Table 102 Configuration via SNMP

STEPS	MIB VARIABLE	VALUE
Step 1	pwTftpServer	Set the IP address of the TFTP server.
Step 2	pwTftpFileName	Set the file name, for example, g3000hcfg.txt.
Step 3	pwTftpFileType	Set to 3 (text configuration file).
Step 4	pwTftpOpCommand	Set to 2 (download).

Verifying Your Configuration File Upload Via SNMP

You can use SNMP management software to display the configuration file version currently on the device by using the following MIB.

Table 103 Displaying the File Version

ITEM	OBJECT ID	DESCRIPTION
pwCfgVersion	1.3.6.1.4.1.890.1.9.1.2	This displays the current configuration file version.

Troubleshooting Via SNMP

If you have any difficulties with the configuration file upload, you can try using the following MIB 10 to 20 seconds after using SNMP to have the AP download the configuration file.

Table 104 Displaying the File Version

ITEM	OBJECT ID	DESCRIPTION
pwTftpOpStatus	1.3.6.1.4.1.890.1.9.1.6	This displays the current operating status of the TFTP client.

Configuration File Format

The text based configuration file must use the following format.

Figure 256 Configuration File Format

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 1 xxx
wcfg security save
wcfg ssid 1 xxx
wcfg ssid save
```

The first line must be `!#ZYXEL PROWLAN`.

The second line must specify the file version. The AP compares the file version with the version of the last configuration file that it downloaded. If the version of the downloaded file is the same or smaller (older), the AP ignores the file. If the version of the downloaded file is larger (newer), the AP uses the file.

Configuration File Rules

You can only use the `wlan` and `wcfg` commands in the configuration file. The AP ignores other ZyNOS commands but continues to check the next command.

The AP ignores any improperly formatted commands and continues to check the next line.

If there are any errors while processing the configuration file, the AP generates a message with the line number and reason for the first error (subsequent errors during the processing of an individual configuration file are not recorded). You can use SNMP management software to display the message by using the following MIB.

Table 105 Displaying the Auto Configuration Status

ITEM	OBJECT ID	DESCRIPTION
pwAutoCfgMessage	1.3.6.1.4.1.890.1.9.1.9	Auto configuration status message string

The commands will be executed line by line just like if you entered them in a console or Telnet CI session. Be careful to ensure the integrity of the whole AP configuration. If there are existing settings in the AP, the newly loaded configuration file will either coexist with the previous settings or replace them.

You can zip each configuration file. You must use the store compression method and a .zip file extension. When zipping a configuration file, you can also add password protection using the same password that you use to log into the AP.

Wcfg Command Configuration File Examples

These example configuration files use the `wcfg` command to configure security and SSID profiles.

Figure 257 WEP Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 11
wcfg security 1 name Test-wep
wcfg security 1 security wep
wcfg security 1 wep keysize 64 ascii
wcfg security 1 wep key1 abcde
wcfg security 1 wep key2 bcdef
wcfg security 1 wep key3 cdefg
wcfg security 1 wep key4 defgh
wcfg security 1 wep keyindex 1
wcfg security save
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 1 l2iolation disable
wcfg ssid 1 macfilter disable
wcfg ssid save
```

Figure 258 802.1X Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 2 name Test-8021x
wcfg security 2 mode  8021x-static128
wcfg security 2 wep key1 abcdefghijklm
wcfg security 2 wep key2 bcdefghijklmn
wcfg security 2 wep keyindex 1
wcfg security 2 reauthtime 1800
wcfg security 2 idletime 3600
wcfg security save
wcfg radius 2 name radius-rd
wcfg radius 2 primary 172.23.3.4 1812 1234 enable
wcfg radius 2 backup 172.23.3.5 1812 1234 enable
wcfg radius save
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 2 qos 4
wcfg ssid 2 l2isolation disable
wcfg ssid 2 macfilter disable
wcfg ssid save
```

Figure 259 WPA-PSK Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 13
wcfg security 3 name Test-wpapsk
wcfg security 3 mode wpapsk
wcfg security 3 passphrase qwertyuiop
wcfg security 3 reauthtime 1800
wcfg security 3 idletime 3600
wcfg security 3 groupkeytime 1800
wcfg security save
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 3 qos 4
wcfg ssid 3 l2siolation disable
wcfg ssid 3 macfilter disable
wcfg ssid save
```

Figure 260 WPA Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 14
wcfg security 4 name Test-wpa
wcfg security 4 mode wpa
wcfg security 4 reauthtime 1800
wcfg security 4 idletime 3600
wcfg security 4 groupkeytime 1800
wcfg security save
wcfg radius 4 name radius-rd1
wcfg radius 4 primary 172.0.20.38 1812 20 enable
wcfg radius 4 backup 172.0.20.39 1812 20 enable
wcfg radius save
wcfg ssid 4 name ssid-wpa
wcfg ssid 4 security Test-wpa
wcfg ssid 4 qos 4
wcfg ssid 4 l2isolation disable
wcfg ssid 4 macfilter disable
wcfg ssid save
```

Wlan Command Configuration File Example

This example configuration file uses the `wlan` command to configure the AP to use the security and SSID profiles from the `wcfg` command configuration file examples and general wireless settings. You could actually combine all of this chapter's example configuration files into a single configuration file. Remember that the commands are applied in order. So for example, you would place the commands that create security and SSID profiles before the commands that tell the AP to use those profiles.

Figure 261 Wlan Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 15
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 4 name ssid-wpa2psk
wcfg ssid 4 security Test-wpa2psk
wcfg ssid save
!line starting with '!' is comment
!change to channel 8
wlan chid 8
!change operating mode -> AP mode,
!then select ssid-wep as running WLAN profile
wlan opmode 0
wlan ssidprofile ssid-wep
!change operating mode -> MBSSID mode,
!then select ssid-wpapsk, ssid-wpa2psk as running WLAN profiles
wlan opmode 3
wlan ssidprofile ssid-wpapsk ssid-wpa2psk
! set output power level to 50%
wlan output power 2
```

G

Legal Information

Copyright

Copyright © 2008 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

H

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

A

access 34
access point 34
access privileges 36
address assignment 141
address filtering 33
administrator authentication on RADIUS 86
Advanced Encryption Standard
  See AES.
AES 278
alternative subnet mask notation 315
antenna 237
  directional 281
  gain 281
  omni-directional 281
AP 33, 34, 35, 145, 271
AP+Bridge 33, 35
applications 33
  Access Point 34
  AP/Bridge 35
  Bridge/Repeater 34
  MBSSID 36
ATC 93, 128
ATC+WMM 128
ATM 93
authentication server 33
auto configuration 321
auto configuration status 324

B

backup 228
Basic Service Set
  see BSS
bridge 34, 35
Bridge Protocol Data Units (BPDUs) 97
Bridge/Repeater 33, 34
BSS 36, 269
BSSID 33

C

CA 276
CAPWAP 51
Certificate Authority
  See CA.
certificates 170
  thumbprint algorithms 178
  thumbprints 178
  verifying fingerprints 178
certifications 329
  notices 330
  viewing 331
channel 33, 271
  interference 271
Class of Service (CoS) 95
command interface 39
configuration 33
configuration file
  examples 324
  format 323
configuration file rules 324
contact information 333
Control and Providioning of Wireless Access Points
  See CAPWAP
copyright 329
CoS 95
CTS (Clear to Send) 272
customer support 333

D

default 230
DFS 97
Differentiated Services 95
DiffServ 95
DiffServ Code Point (DSCP) 95
DiffServ Code Points 95
DiffServ marking rule 95
disclaimer 329
DS field 95
DSCPs 95
Dynamic Frequency Selection 97

dynamic WEP key exchange 277

E

EAP authentication 275
encryption 35, 278
ESS 270
ESSID 236
Extended Service Set
see ESS
Extended Service Set IDentification 101, 125

F

FCC interference statement 329
file version 323
filtering 33
firmware file
maintenance 225
fragmentation threshold 272
friendly AP list 148
FTP 39, 151, 155
restrictions 151

G

general setup 85
guest SSID 37

H

hidden node 271
honeypot attack 146
host 87
HTTPS 156
example 158
humidity 237

I

IANA 320
IBSS 269
IEEE 802.11g 273
IEEE 802.1x 33
in-band management 207
Independent Basic Service Set 225
see IBSS
initialization vector (IV) 278
installation 33
interference 33
internal authentication server 33
Internet Assigned Numbers Authority
See IANA
Internet security gateway 33
Internet telephony 36
IP address 141, 142, 238
IPSec VPN capability 239
isolation 33

L

layer-2 isolation 33, 37
log descriptions 198
logs 195

M

MAC address 33, 134
MAC address filter action 135, 136
MAC filter 37, 134
MAC filtering 239
MAC service data unit 100, 105, 124
maintenance 33
management 33
Management Information Base (MIB) 163
management VLAN 207
managing the device
good habits 40
using FTP. See FTP.
using Telnet. See command interface.
using the command interface. See command interface.
max age 97
MBSSID 33, 36
Message Integrity Check (MIC) 278
mobile access 33
mode 33
MSDU 100, 105, 124

N

NAT 320
network 33
network access 33
network bridge 34
network traffic 33

O

operating mode 33
out-of-band management 207

P

Pairwise Master Key (PMK) 278, 279
password 86, 238
path cost 96
Per-Hop Behavior 95
PHB (Per-Hop Behavior) 95
PoE 241
power specification 237
power specifications 241
preamble mode 273
pre-configured profiles 37
priorities 93
prioritization 33
private IP address 141
product registration 331
PSK 278

Q

QoS 33, 128
Quick Start Guide 43

R

radio 33
RADIUS 274
  message types 275
  messages 275
  shared secret key 275
rapid STP 96
reauthentication time 114, 115, 116, 117, 118
registration
  product 331
related documentation 3
remote management
  how SSH works 152
  HTTPS 156
  HTTPS example 158
  SSH 152
  SSH implementation 153
  Telnet 153
remote management limitations 151
repeater 34
restore 228
RF interference 33
roaming 137
  requirements 138
rogue AP 33, 145, 146, 147, 148, 149
rogue AP list 149
root bridge 96
RTS (Request To Send) 272
  threshold 271, 272
RTS/CTS handshake 100, 105, 124

S

safety warnings 6
security 34
security profiles 33
server 33
Service Set 101, 125
Service Set Identifier
  see SSID
SNMP 162, 239
  manager 163
  MIBs 164
  traps 165
  version 3 and security 165
Spanning Tree Protocol 96
specifications 241
SSH 152
  how SSH works 152
  implementation 153
SSID 36
SSID profile 127
  pre-configured 36
SSID profiles 36, 37
STP 96

STP - how it works 97
STP (Spanning Tree Protocol) 239
STP path costs 96
STP port states 97
STP terminology 96
subnet 313
subnet mask 238, 314
subnetting 316
syntax conventions 4
system name 85
system timeout 152

T

tagged VLAN example 207
Telnet 153
telnet 153
temperature 237
Temporal Key Integrity Protocol (TKIP) 278
text file based auto configuration 239, 321
TFTP restrictions 151
time setting 88
time-sensitive 33
ToS 95
trademarks 329
traffic security 33
Type of Service 95

U

use 33

V

Virtual Local Area Network 203
VLAN 203
VoIP 33, 36, 128
VoIP SSID 37

W

warranty 331
  note 331
wcfg command 324
WDS 34, 35, 101
web 157
web configurator 33, 43, 45
WEP 33
WEP encryption 113
Wi-Fi Multimedia QoS 92
Wi-Fi Protected Access 33, 277
wired network 33, 34
wireless channel 236
wireless client WPA supplicants 279
Wireless Distribution System (WDS) 35
wireless Internet connection 34
wireless LAN 236
wireless security 36, 236, 273
WLAN
  interference 271
  security parameters 280
WLAN interface 33
WMM 128
WPA 33, 277
  key caching 278
  pre-authentication 278
  user authentication 278
  vs WPA-PSK 278
  wireless client supplicant 279
  with RADIUS application example 279
WPA2 33, 277
  user authentication 278
  vs WPA2-PSK 278
  wireless client supplicant 279
  with RADIUS application example 279
WPA2-Pre-Shared Key 277
WPA2-PSK 277, 278
  application example 279
WPA-PSK 277, 278
  application example 279